Documentation

HiPath Cordless IP

Service Manual

A31003-C1010-S100-4-7620

Communication for the open minded

Siemens Enterprise Communications
www.siemens-enterprise.com

SIEMENS

Communication for the open minded

Contents

Contents

Contents

List of Tables

List of Figures

1 Introduction and Important Notes

1.1 Safety Information and Warnings

Work on communication systems and devices may **only** be carried out by qualified persons.

For the purposes of safety information and warnings, qualified persons are persons who are authorized to place into operation, ground, and label systems, devices, and lines in accordance with applicable safety procedures and standards.

It is absolutely essential that you read and understand the following safety information and warnings before starting installation and implementation work on the communication system or device.

You should also carefully read and observe all safety information and warnings on the communication systems and devices themselves.

Familiarize yourself with emergency numbers.

Types of safety information and warnings

The following grades of safety information/warnings are used in this manual:

⚠ **DANGER**

Indicates an immediate danger that could result in death or serious injury.

⚠ **WARNING**

Indicates a general danger that could result in death or serious injury.

⚠ **CAUTION**

Indicates a danger that could result in injury.

NOTE: Indicates situations that could result in damage to property and/or loss of data.

Symbols for specifying the source of danger more exactly

The following symbols are not usually used in the manual. They explain symbols that may be depicted on the communication systems and equipment.

Electricity Weight Heat Fire Chemicals ESD* Laser

* electrostatically sensitive devices

1.2 Correct Use

The communications system may only be used for the purpose described in this document and only in connection with the additional devices and components as recommended and permitted by
Siemens Enterprise Communications GmbH & Co. KG under Trademark License of Siemens AG 2008.
The proper use of the communications system assumes correct transport,storage, assembly and setup as well as careful operation and maintenance.

1.3 Proper disposal and recycling

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service, the shop where you purchased the product or your sales representative.

The statements quoted above are only fully valid for equipment which is installed and sold in the countries of the European Union and is covered by the directive 2002/96/EC. Countries outside the European Union may have other regulations regarding the disposal of electrical and electronic equipment.
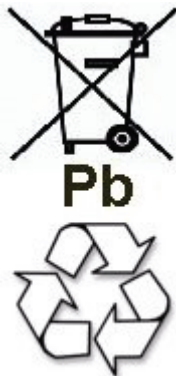
Used accumulators and batteries with this sign are valuable economic goods and must be recycled. Used accumulators and batteries that are not recycled must be disposed of as hazardous waste with full observance of all regulations.

1.4 Standards and Guidelines on Installation

1.4.1 Labeling

	This device complies with the EU guideline 1999/5/EEC as confirmed by the CE certificate.

	This device has been manufactured in accordance with our certified environmental management system (ISO 14001). This process ensures that energy consumption and the use of primary raw materials are kept to a minimum, thus reducing waste production.

1.5 Data Protection and Data Security

This system processes and uses personal data for purposes such as call detail recording, displays, and customer data acquisition.

In Germany, the processing and use of such data is subject to various regulations, including those of the Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG). For other countries, please follow the appropriate national laws.

The aim of data protection is to protect the rights of individuals from being adversely affected by use of their personal data.

In addition, the aim of data protection is to prevent the misuse of data when it is processed and to ensure that one's own interests and the interests of other parties which need to be protected are not affected.

The customer is responsible for ensuring that the system is installed, operated and maintained in accordance with all applicable labor laws and regulations and all laws and regulations relating to data protection, privacy and safe labor environment.

Employees of Siemens Enterprise Communications GmbH & Co. KG are bound to safeguard trade secrets and personal data under the terms of the company's work rules.

In order to ensure that the statutory requirements are consistently met during service – whether on-site or remote – you should always observe the following rules. You will not only protect the interests of your and our customers, you will also avoid personal consequences.

A conscientious and responsible approach helps protect data and ensure privacy:

• Ensure that only authorized persons have access to customer data.

• Take full advantage of password assignment options; Never give passwords to an unauthorized person orally or in writing.

• Ensure that no unauthorized person is able to process (store, modify, transmit, disable, delete) or use customer data in any way.

• Prevent unauthorized persons from gaining access to storage media, such as backup CDs or log printouts. This applies to service calls as well as to storage and transport.

• Ensure that storage media which are no longer required are completely destroyed. Ensure that no sensitive documents are left unprotected.

Work closely with your customer contact; this promotes trust and reduces your workload.

1.6 Documentation Feedback

If you have questions that are not answered by this document:

• Internal employees should contact their National Support Center.

• Customers should contact their retailer or the Siemens Customer Support Center.

When you call, state the title, ID number, and issue of the document.

Example:

• **Title:** HiPath Cordless IP, Service Documentation

• **ID number:** A31003-C1010-S100-1-7620

• **Issue:** 1

2 Overview

The HiPath Cordless IP solution extends the scope of the DECT standard introduced for voice communication, making it now available for Voice over IP infrastructures.

The radio range covered by the HiPath Cordless IP system is made up of DECT IP base stations that together form either an seamless network of overlapping and synchronous radio cells or individual radio islands. The size of a radio cell depends on local/structural factors.

Voice over IP infrastructures are connected via the SIP protocol. In their capacity as mobile communication solutions, DECT radio cells are therefore an optimal enhancement to SIP-compliant Voice over IP systems.

The DECT IP base stations support seamless handover in ongoing voice connections, that is, moving from one radio cell to another during a call with a DECT handset. The roaming function is also available for mobile stations.

HiPath Cordless IP also supports the DECT protocol GAP (Generic Access Profile) and the radio protocol PN-CAP. The basic function scope required by ETSI is thus extended to include a number of Siemens-specific features.
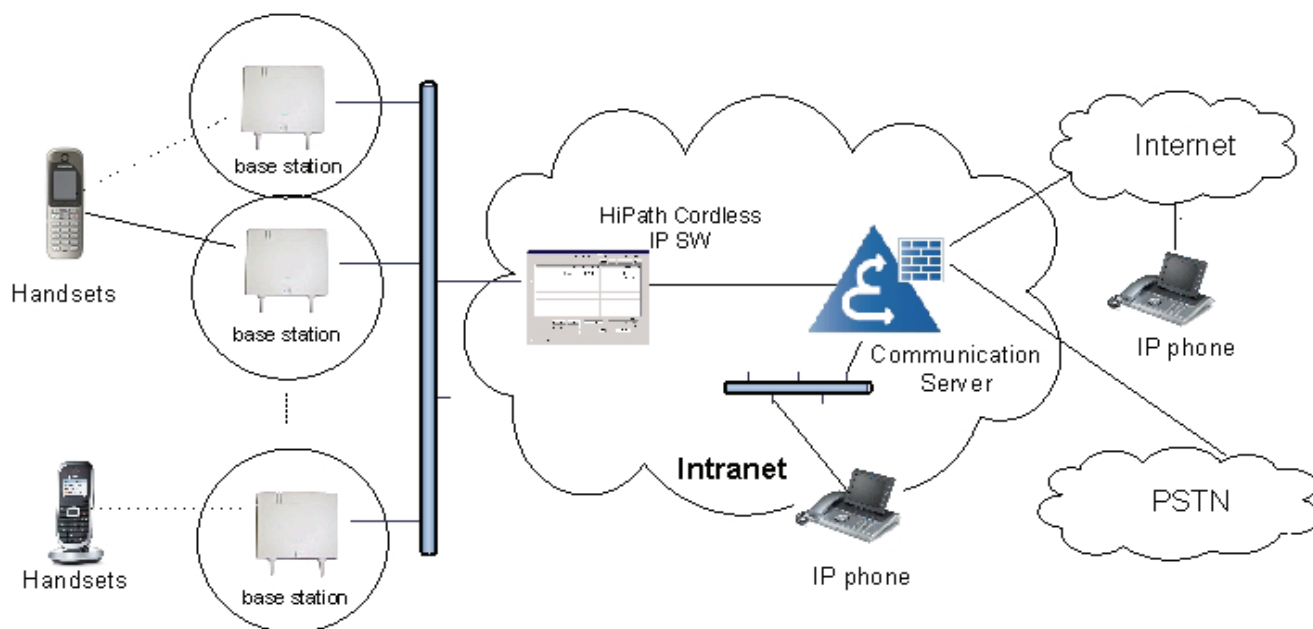
Figure 1   *General Overview of the HiPath Cordless IP System*

The HiPath Cordless IP System contains the following main components, see also Figure 1:

- **Handset**: Gigaset professional DECT handsets with PN-CAP functionality

- **BSIP1**: DECT IP Basestations with GAP/ PN-CAP functionality to the handset and IP interface to the Ethernet network.

- **HiPath Cordless IP SW**: central Server SW component for control of the DECT IP Basestations, SIP interworking with the communication server, and the common administration and configuration interface of the whole HiPath Cordless IP solution. The HiPath Cordless IP Server SW can either be located on one of the DECT IP Basestations or on a dedicated Server HW.

2.1 Einleitung

The HiPath Cordless IP solution is designed as a DECT system with an SIP interface to the communication server.

2.1.1 DECT IP Base Station (BSIP1)

DECT IP base stations combine to form a network of radio cells. Roaming between radio cells is possible for DECT handsets during a voice connection if the radio cells are synchronized and overlap.

DECT IP base stations come with all necessary software for the DECT and IP functions. This software is configured and administered via the HiPath Cordless IP SW.

2.1.2 HiPath Cordless IP SW

HiPath Cordless IP SW is installed once on a system and can be activated on a DECT IP base station or can be installed on a server HW. It supports the following functions:

Function: Router and protocol converter

The HiPath Cordless IP SW serves as the interface between the IP DECT base stations and the communication server.

It manages the voice connections between the communication server and the relevant DECT IP base station and converts these into a data format that can be reed by the DECT IP base stations. At DECT layer the media packets are enhanced with DECT signaling (time frame, frequency) information. The HiPath Cordless IP SW converts incoming RTP media data into UDP packets via DECT codec G726.

Only HiPath Cordless IP SW knows, at which DECT IP Basestation a special DECT handset is located. For the communication server or any other phone, the HiPath Cordless IP SW is the endpoint. Whenever a handset performs a handover, this process is invisible outside the HiPath Cordless IP System. In the view of the communication server the HiPath Cordless IP SW is like a Gateway User-Agent that manages lots of handsets. Handsets use the HiPath Cordless IP SW for registration at the communication server. This software regulates the check-in procedure for the DECT handsets and their management.

Function: Configuration and administration interface

All administrative functionality for the DECT IP Basestations as well as for HiPath Cordless IP SW itself is performed via a Web Based Management to the HiPath Cordless IP SW, i.e., all DECT IP Basestations are administered via HiPath Cordless IP SW.

Function: Synchronization management

DECT IP base stations must be perfectly synchronized as a prerequisite for seamless handover. If the DECT IP base stations are synchronized, they combine to form a seamless handover cluster. The synchronization management function only works in this cluster. Additional clusters are possible but not synchronized. Seamless handover is not possible between different asynchronous clusters.

In DECT systems with line-switched connections such as HiPath Cordless systems, the synchronization information needed for synchronizing the DECT IP base stations is obtained from the UP0 connection. This is not possible in the HiPath Cordless IP system.

DECT-based synchronization ("synchronization over the air")

This method to synchronize overlapping radio cells runs under SW control within the DECT part of the DECT IP Basestation. The HiPath Cordless IP SW is acting only as admin point that notices when a base station has lost its synchronization.

The DECT IP base station must be located in the overlap area of the DECT IP base station that it wants to synchronize with over the DECT interface. For every DECT IP Basestation the synchronization "Master" have to be configured by the configuration Interface of the HiPath Cordless IP SW. DECT information for synchronization are exchanged directly between the DECT IP Basestations.

A DECT IP base station can also be synchronized with other DECT IP base stations as this increases the synchronism available in the cluster. It is important to avoid synchronization loops.

In the event of loss of synchronization, the DECT IP base station stops accepting calls once all ongoing calls that were being conducted on the asynchronous DECT IP base station have ended and then it re-synchronizes the asynchronous DECT IP base station.

LAN-based synchronization

A DECT IP base station can be synchronized over LAN with another DECT IP base station. The IEEE standard Precision Time Protocol (PTP) IEEE1588 is used for this. In contrast to DECT-based synchronization, LAN-based synchronization uses only one DECT IP base station in the cluster as the clock master for the other DECT IP base stations to be synchronized. This PTP master sends out multicast messages with time information. The slaves send back modified time messages to the master.

In contrast to over-the-air synchronization, LAN-based synchronization requires less configuration.
On the other hand, high demands are placed on Ethernet characteristics such as symmetry, packet loss, delay, jitter (primarily delay variation). All of the Ethernet components involved (especially the switches) therefore have to fulfill special

requirements. If thresholds are exceeded (primarily jitter), this leads to loss of synchronization, which in turn leads to a resynchronization process. No calls can be conducted on the relevant DECT IP base station during this process.

PTP messages are exchanged only between the DECT IP Basestations, the HiPath Cordless IP SW is not involved.

DECT IP Basestations who are e.g. separated by iron doors cannot synchronize each other over the air can use instead PTP.

For PTP, the underlying network must fulfill some restrictions like very little delay, i.e., no routers or NAT devices (see chapter Section 2.4).

A combination of air and LAN synchronization is possible in a cluster of synchronous DECT IP base stations.

Advantages of LAN synchronization compared with over-the-air synchronization:

- Greater flexibility in the arrangement of the base stations as no synchronization chains need to be formed.

- Fewer DECT IP base stations required as the overlapping area of the DECT IP base stations is smaller.

- Configuration of the system is simplified as all DECT IP base stations can be synchronized on one synchronization master.

In the event of loss of synchronization, the DECT IP base station stops accepting calls once all ongoing calls that were being conducted on the asynchronous DECT IP base station have ended and then it re-synchronizes the asynchronous DECT IP base station.
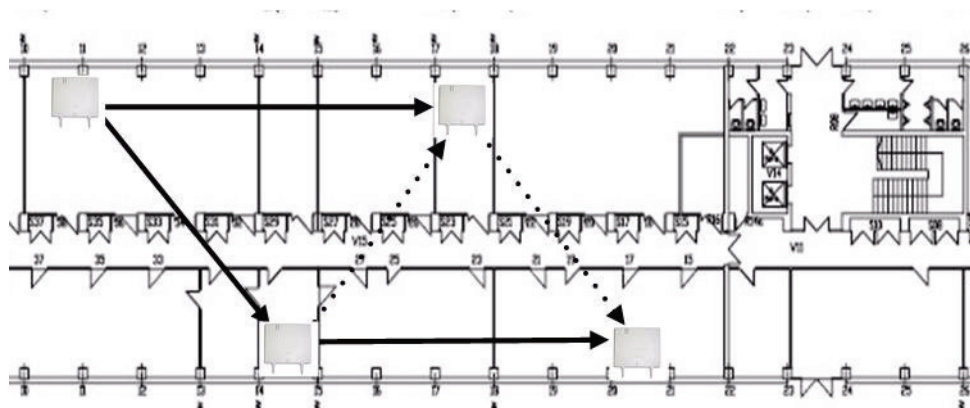
Figure 2   Optimum system synchronization over DECT at synchronization over the air

 Standard synchronization

 Alternative synchronization if standard synchronization fails
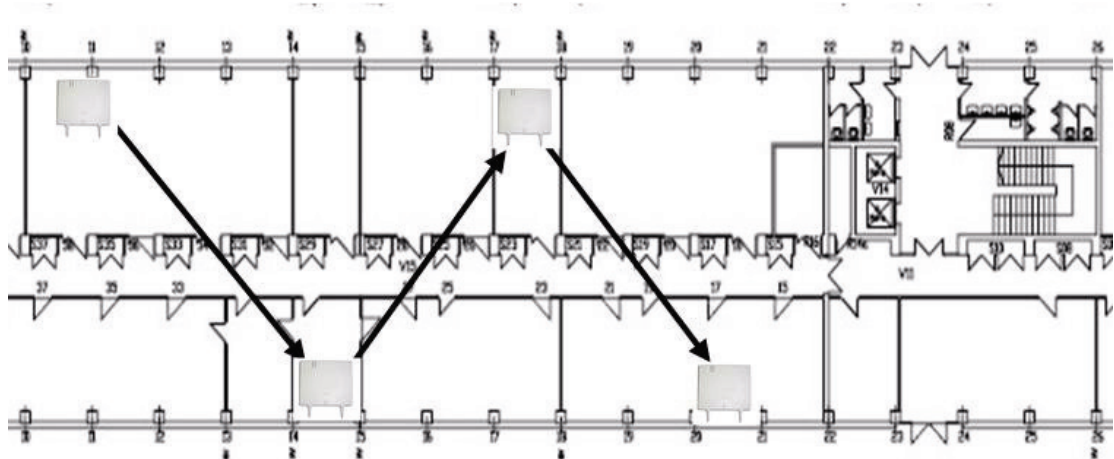
Figure 3   *Not optimally synchronized, each DECT IP base station has only one synchronization partner*
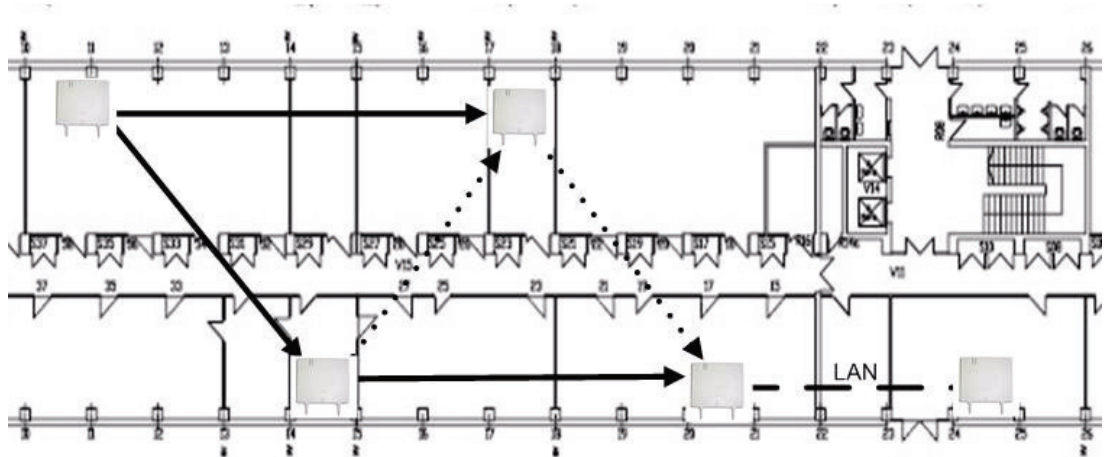
Figure 4   *The two lower DECT IP base stations are synchronized over LAN because a solid fire door prevents DECT-based synchronization. The quick passage of data through a fire door cannot always guarantee reliable DECT synchronization.*

This data is transported in a VPN tunnel to ensure that the signaling and voice data in active voice connections between a DECT IP base station and HiPath Cordless IP software is protected against manipulation and interception. For the VPN encryption IPSec is used.

The DECT IP base stations are set up in communication with the HiPath Cordless IP SW. As soon as a new DECT IP base station is connected to the Ethernet, it starts to send multicast packets with its MAC address. The HiPath Cordless IP SW then activates and takes over control of the DECT IP base station. The HiPath Cordless IP SW then sends the DECT IP base station an IP address for communication purposes as well as its own IP address as a future target address for data traffic.

2.1.2.1 Communication Interfaces

The following picture gives an overview of the protocols used between DECT Handset, DECT IP Basestation, HiPath Cordless IP SW and the communication server.
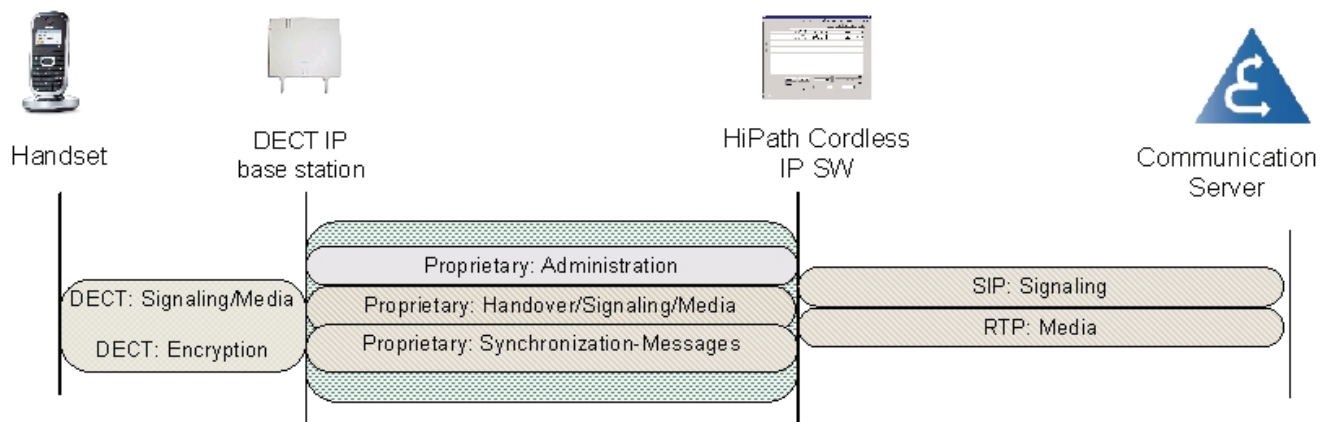
Figure 5   Protocols of the path between Handset and Communication Server
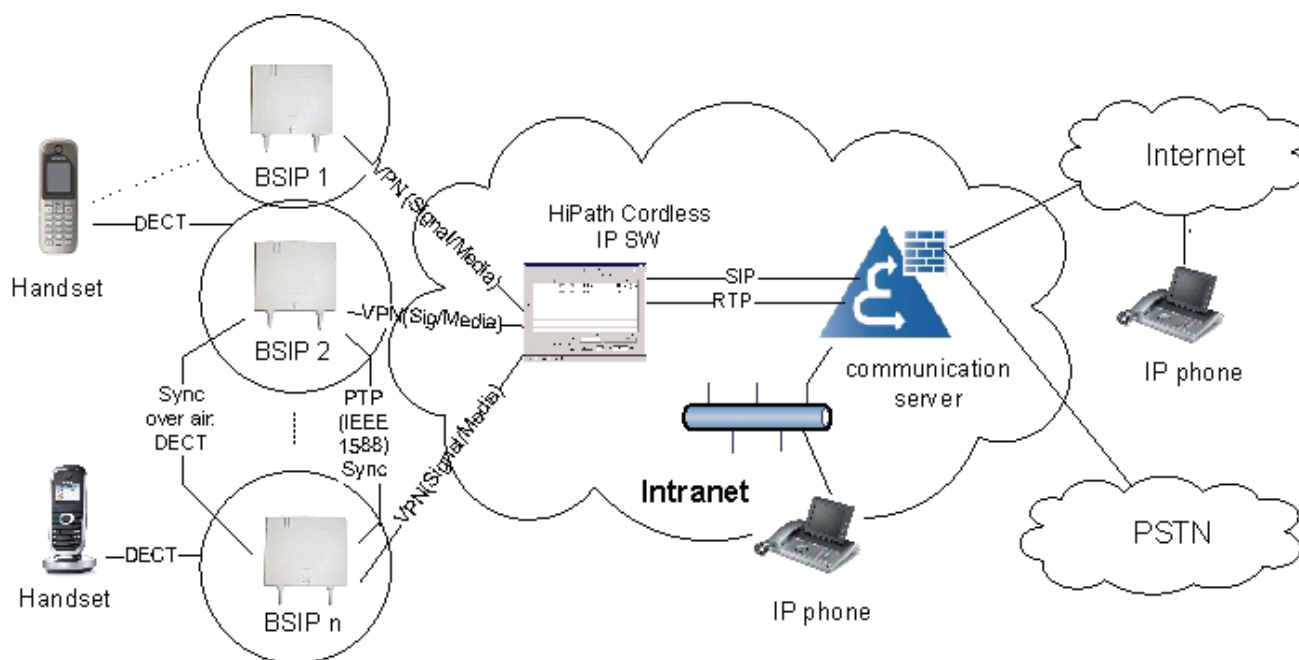
Figure 6   Depicts all communication channels of the HiPath Cordless IP System

The following list gives an overview of all communication-channels within the HiPath Cordless IP System:

DECT Handset - User: Gigaset professional DECT Handsets with PN-CAP functionality

DECT Handset - DECT IP Basestation (BSIP1): In this multicell DECT system, a call can be handed over seamlessly from one BSIP1 to the other. If seamless handover is impossible and the signal quality is decreasing, at a certain point the handset can send a warning tone and the connection breaks off.

DECT IP Basestation (BSIP1) - DECT IP Basestation (BSIP1): An accurate synchronization is needed between DECT IP Basestation for seamless handover.

DECT IP Basestation (BSIP1) - HiPath Cordless IP SW: the DECT IP Basestation (BSIP1) is able to handle a tunnel to the HiPath Cordless IP SW, in which the voice data of all active calls and all signaling data is transported. The connection between BSIP1 and HiPath Cordless IP SW is system-specific, i.e., this protocol is IP based and uses UDP packages both ways.

HiPath Cordless IP SW - communication server: The SIP interface between the HiPath Cordless IP SW and the communication server is standard based. Seen from the communication server the DECT over IP System is a set of SIP subscribers represented by a GW User-Agent, which is the HiPath Cordless IP SW connected to the DECT handsets, i.e. the subscribers are the DECT handsets.

2.2 System Configuration

There are two main scenarios for installing the HiPath Cordless IP solution:

- The HiPath Cordless IP SW is activated on one of the DECT IP base stations.

- The HiPath Cordless IP SW is installed on a server.

In both cases, all voice and signaling data (RTP/SIP) are always routed over the HiPath Cordless IP SW because this is the only software that supports a routing and protocol converter function.

Scenarios are also possible where the HiPath Cordless IP SW is installed a number of times per communication server. Such scenarios do not support seamless handover between the different clusters formed with synchronous DECT IP base stations. Cascading is not available at present for communication server software.

2.2.1 Scenario 1 - HiPath Cordless IP SW is activated on a DECT IP base station

All DECT IP base stations always also support the same functions as HiPath Cordless IP SW. This means that in principle, all DECT IP base stations can perform HiPath Cordless IP SW functions in addition to the actual DECT functionality. The HiPath Cordless IP SW must be activated before the DECT IP base station can perform this function.

The following system limits apply in this scenario based on resource availability in BSIP1:

- up to 10 DECT IP base stations

- up to 10 parallel calls

These system limits apply to each cluster of synchronous DECT IP base stations where seamless handover is possible. Up to 99 Gigaset professional mobile devices can be configured in the data base of the HiPath Cordless IP SW and up to 55 of these mobile devices can be logged on to the Communication Server.

2.2.2 Scenario 2 - HiPath Cordless IP SW is installed on dedicated server hardware

The HiPath Cordless IP SW is installed on a server. The requisite operating system for the server is Linux Distribution openWRT. Both the server and the entire software on the server are included in the HiPath Cordless IP solution's scope of features.

The following system limits apply in this scenario:

- – up to 60 DECT IP base stations

- – up to 50 parallel calls

These system limits apply to each cluster of synchronous DECT IP base stations where seamless handover is possible. Up to 100 Gigasets can be configured in the HiPath Cordless IP software.

2.3 DECT IP Base Station Data

Table 1   Technical data DECT IP base station

Parameter	DECT IP base station BSIP1	Outdoor case
DECT Interface		
Max. amount of DECT channels	120	
DECT Signalling	GAP/ PN-CAP	
IP Interface		
Network connection	Ethernet 10/100 Base T	
PoE class	Class 2 according IEE802.3af	
Power consumption	< 6,5 W; PoE Class 2	
Max. Voice channels	12 (bei G.711)	
Codecs	G.711/ G.726	
QoS	802.1 p/q	
Echo Cancellation	yes	
DHCP Option	DCHP on or local entry of IP addresses	
SW Distribution	SW Download/ Update central via HiPath Cordless IP SW	
Miscellaneous		
Dimensions (W x H x D in mm)	202 x 256 x 90	296 x 256 x 90
Weight	ca. 0,5 kg	ca. 1,0 kg

Table 1   *Technical data DECT IP base station*

Parameter	DECT IP base station BSIP1	Outdoor case
Operating Temperature	Indoors: 0 ^{o}C bis + 40 ^{o}C	Outdoors (with outdoor housing): - 25 ^{o}C bis + 40 ^{o}C
Storage temperatur range	-5 ^{o}C bis + 45 ^{o}C	
Relative humidity	–	bis 95 %

Figure 7   *DECT IP base station BSIP1 (Item number: U30807-S5494-X)*

2.3.1 Outdoor Case

A DECT IP base station must be installed in a weatherproof outdoor case to guarantee radio coverage in outdoor areas, for example on factory sites. The outdoor case is suitable for mounting on house walls, roofs or masts.

The outdoor case already used for the HiPath Cordless base station BS4 is also used for DECT IP base stations (part number: S30122-X7469-X2).

If using the DECT IP base station outdoors, lightning and overvoltage protection must be provided and guaranteed for the DECT IP base station itself as well as for the feeder into the DECT IP base station and the building. In compliance with EN 61000-4-5, the power supply inlet on the DECT IP base station offers up to 0.5 KV overvoltage protection.
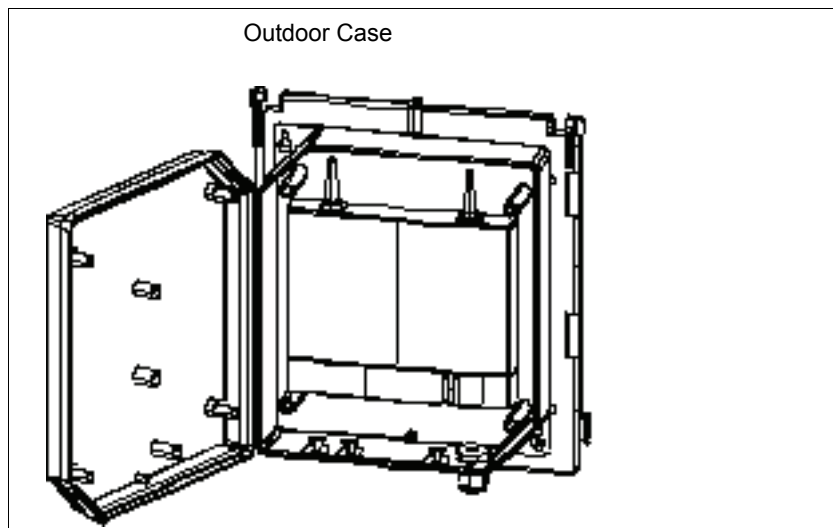
Outdoor Case

Figure 8   *Outdoor case with DECT IP base station*

2.3.2 Powering the DECT IP Base Stations

The DECT IP base station can be powered in two different ways:

- Power-over-Ethernet (PoE) Class 2 to 802.3af

- Power-over-Ethernet: PoE injectors

A PoE injector is used if PoE cannot be made available in the network. The PoE injector must be 802.3af-compatible. Pre-tested and released PoE injectors are available as optional features within the scope of the HiPath Cordless IP solution.

The IEEE802.3af standard allows the PoE Injector to be in any location between the switch and the BSIP1. The maximum allowed distance between the switch and the BSIP1 for IEEE802.3 compliance is 100 m. It is typical to deploy the PoE Injector close to the switch, since by doing this one can use a single UPS (central power supply) to backup both the switch and the PoE Injector.

If overall efficiency is more important than centralized backup and/or management, it makes sense to place the PoE Injector closer to the BSIP1, since the power dissipated at the cable between the PoE Injector and the BSIP1 is directly proportional to the length of this cable ($P = I^2 * R$).

Figure 9   PoE Injector

2.4 Network Requirement

Voice connections only work properly over IP networks if the IP network satisfies all general VoIP network requirements in terms of delay, loss and guaranteed quality of service features.

The following conditions should also be assured for the DECT IP base stations and the HiPath Cordless IP SW in the IP network:

- they have to be part of the same Ethernet segment, a layer-3 routing via an IP router is not supported,

- no devices use the Network Address Translation (NAT) Ethernet segment

- Minimum 2 priority classes acc. to IEEE 802.1 p/q in the IP Network possible

- Use of 100 Mbps full duplex for all switched LAN ports

- as the solution operates with standard IP addresses, these must be freely available in the IP network. Refer to Chapter 5.2.1 for this IP address.

Failure to satisfy these conditions can result in delays in the IP network. This leads to synchronization and voice quality problems in the DECT handsets.

2.5 Software License Management

SW component licensing is only relevant if the HiPath Cordless IP SW is installed on dedicated server hardware. If the HiPath Cordless IP SW is activated on a DECT IP base station, licensing is not performed for the software components of HiPath Cordless IP systems. The SW licensing of the communication server's SIP stations is dependent on this.

If the HiPath Cordless IP SW is located on a dedicated Server HW the number of DECT IP Basestation within the system and the HiPath Cordless IP SW itself in Version 1 is licensed.

The number of DECT IP base stations configured and registered in the HiPath Cordless IP SW is counted for this. The HiPath Cordless IP SW is also counted in version 1.

HiPath License Management (HLM) is used in the HiPath Cordless IP SW. The Siemens licensing process consists of 4 different steps, see for a general overview Figure 10:

1. The license key is centrally created and contains the number of DECT IP Basestations in the system and the number of HiPath Cordless IP SW in Version 1. The license file is signed by Siemens CA.

2. The license file is being download from a License Server (CLS, Central License Server). In general, the Customer Site Components (CSC) are part of the license SW of the product that interpret the license file and distribute it in a customer's network. In detail, the Customer License Agent (CLA) - usually on the Siemens communication server - connects to the License Server and downloads the license file. Via CLA the customer can monitor the usage of licenses.

    If the CLA is located on the Siemens communication server, the license file is downloaded onto the Siemens communication server. A Customer License Client (CLC) which is always on HiPath Cordless IP SW, is told, under which link on the Siemens communication server it can contact the CLA.

    In case the customer's network does not have a Siemens communication server the HiPath Cordless IP SW itself will also be provided with CLA SW and the license file will be downloaded directly onto the HiPath Cordless IP SW. The CLC is told that the files are on the same server.

3. Verification of the license key: the license file is read in and the signature is checked. If the check is successful, the license data will be retrieved from the license file. This is done by CLA.

4. License Enforcement: the license conditions are checked and supervised in the running system, e.g., as soon as a DECT IP Basestation is installed and added to the system, the CLC contacts the CLA and a license counter in the license file is decremented. This step is performed by the Customer License Client (CLC) that is always running on HiPath Cordless IP SW.

Figure 10 shows the HiPath Cordless IP license management as part of the HiPath License Management (HLM). CLS is the Central License Server. CLA is usually installed on the same Server as the Siemens communication server. In HiPath Cordless IP SW the CLC module is integrated, which is the interface to the CLA.
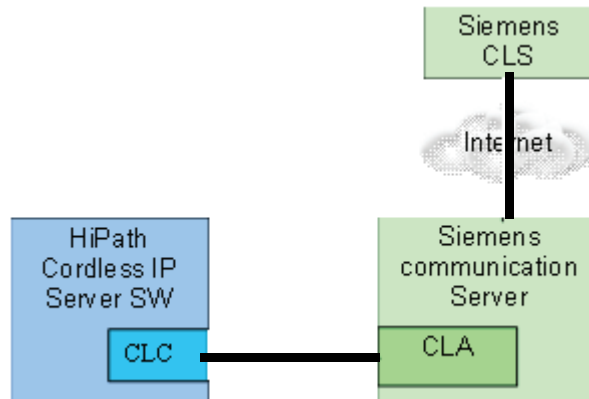
Figure 10   HiPath Cordless IP SW: License Management

When the HiPath Cordless IP System is setup at a customer, a special Grace Period starts, i.e. the product can be used for 30 days without a license. Within this period of time, the one who is installing the system has to get a valid product license. After installation of the license software on the system, this license has no more time restrictions.

For more information on HiPath License Management, refer to the manual "License Management V1.0, User Manual", Ref.No.: A31003-H2510-B100-*-7619.

3 Planning a HiPath Cordless IP System

When planning a cordless system, the position of the base station is critical for system performance. The load should be optimized using locations with a high call volumes and radio coverage.

3.1 Planning According to Call Traffic Load

- The borders of base station radio cells should not be located in high traffic areas because changing base stations during a call (handover) increases traffic load.

- The best base should be as unique as possible to avoid frequent switching.

Recommended number of DECT users (number of simultaneously registered users) for 10 voice channels in accordance with the volume of traffic (Erlang value).

10 Voice channels with 100 mErl/user (low traffic)		
Grad of Service (GoS)	0,1 %	1 %
Traffic	3,09 Erl	4,46 Erl
User	31	45
10 Voice channels with 150 mErl/user (normal traffic)		
Grad of Service (GoS)	0,1 %	1 %
Traffic	3,09 Erl	4,46 Erl
User	21	30
10 Voice channels with 200 mErl/user (high traffic)		
Grad of Service (GoS)	0,1 %	1 %
Traffic	3,09 Erl	4,46 Erl
User	15	22

Table 2   Recommended amount of users at 10 voice channels

Recommended number of DECT users (number of simultaneously registered users) for 50 voice channels in accordance with the volume of traffic (Erlang value).

50 Voice channels with 100 mErl/user (low traffic)		
Grad of Service (GoS)	0,1 %	1 %
Traffic	32,51 Erl	37,90 Erl
User	325 *	379 *
50 Voice channels with 150 mErl/user (normal traffic)		
Grad of Service (GoS)	0,1 %	1 %
Traffic	32,51 Erl	37,90 Erl
User	217	253
50 Voice channels with 200 mErl/user (high traffic)		
Grad of Service (GoS)	0,1 %	1 %
Traffic	32,51 Erl	37,90 Erl
User	163	190

Table 3   Recommended amount of users at 10 voice channels

(*) Zur Zeit ist eine Gesamtanzahl von max. 100 Gigaset professional (Teilnehmern) möglich, obwohl theoretisch eine größere Anzahl von Gigaset prof. gemäß Verkehrswert möglich wäre.

3.2 General

DECT IP Base station (BSIP1)

DECT IP base stations are logically connected to the HiPath Cordless IP server software over LAN connections. This software is connected to the communication server via the SIP interface.

- Base station range

    – Ethernet cable range (see also Chapter 2.4 for network requirements between DECT IP base stations and the HiPath Cordless IP server software)

    – Spatial distance
      The distance which must be maintained between the different installation points of the base stations is dependent on

        – the range

        – the traffic capacity of the radio cells.
          You can increase the number of simultaneous calls in a radio cell by overlapping radio cells (overload).

        – Distance
          For synchronization over DECT, the DECT IP base stations you want to synchronize with each other must be able to exchange their management information (beacons). For this to work, they must be located in the areas where their radio cells overlap.
          This does not apply for use of over-the-air synchronization.

    – Overlap areas inside/outside buildings (see following chapter), measurement results (RSSI points) (see Section 7.2.1)

Radio measurement techniques are used to determine the radio range of DECT IP base stations.

   DECT IP base stations inside buildings

    – Please note that the base station's connection cable can be repositioned as necessary (connection cable plus reserve loop to be factored in).

   DECT IP base stations in areas outside buildings (e.g. campuses).

    – The base station must be installed in the outdoor case for use is exterior areas.

    – Make sure that adequate lightning and overvoltage protection is provided for the cable feeder into the building and the DECT IP base station

- Radio propagation

   Radio propagation is negatively influenced by

– obstructions with strong absorption qualities (brick walls, dividing walls, ceilings, furniture, steel cabinets, bathroom units, elevators, wire-reinforced glass, leaded windows, blinds and others)

– reflective stationary obstructions (brick buildings, reinforced concrete buildings, buildings with metal sheathing)

– reflective moving obstructions (people, animals, vehicles)

3.3 Propagation Conditions for Radio Traffic

Radio wave propagation in the DECT frequency range is quasioptical. This means that a wave is hindered in its propagation if it hits a solid surface and is thereby reflected to a greater or lesser extent. This reflection is dependent on the physical qualities of the medium.

In the case of conductive materials, the penetration depth into the medium is determined mainly by the magnetic quality and the electrical conductivity.

• Metals with a high degree of conductivity
  These include copper or steel and prevent most DECT frequency radio waves from penetrating, reflecting them in the same way as a mirror reflects light.

• Modern construction materials (exceptions, see above)
  These have relatively poor conductivity levels with the result that electromagnetic waves, even if attenuated, still can pass through.
  Thus, radio traffic is possible within and through buildings.

• Attenuation qualities
  of the construction materials vary greatly resulting in different ranges depending on the propagation direction and the construction material penetrated.

  – Wood (dry and unprocessed),
    glass, plastics (N-conductor)   negligible attenuation

  – Brick walls,
    wood (damp and processed, for example,   medium range of attenuation
    particle board)

  – Reinforced concrete, glass with metal   greatest attenuation
    reinforcement/coating

  This attenuation is mitigated by openings, especially by windows in the buildings as long as they do not have wire-reinforced or metal-plated glass.

The different levels of radio propagation give rise to various scenarios in which radio cells are formed:

• in the open with visibility

• industrial sites with reinforced concrete buildings and buildings with metal facades

- indoor areas in buildings made of brick and light construction materials

- indoor areas in reinforced concrete buildings with diverse interior layout, for example.

3.3.1 In the Open with Visibility

In this scenario, the electromagnetic waves are subject to the lowest amount of attenuation with the result that they produce the greatest radio wavelength.

In principle, base stations in such a scenario produce a radio coverage range with a radius of up to 300 m.

This, however, is usually not possible, since trees, bushes and moving obstructions, such as, people, animals, and vehicles in the direct propagation route can significantly reduce propagation.

NOTE: A base station installed in an attic directly beside a dormer window (no metal reinforcement in the window pane) is the alternative to the outdoor housing for coverage of the outdoor area.
Choose the mounting location carefully:
The base station is often exposed to extreme environmental temperatures, for example, direct sunlight or extreme cold.

3.3.2 Industrial Sites

Buildings of varying structural materials may be found here, including those:

- of light construction materials,

- of brick,

- of reinforced concrete,

- with metal facades.

The distances between the buildings, however, are rarely greater than 100 m. In this scenario, outdoor base stations are practical for covering the outdoor area.

- Buildings of brick or light construction materials
  are generally penetrable, but the magnetic field reception behind the walls is extremely low, resulting, quasioptically, in a shadowed area.

  For example, in the case of a base station installed on the southern side of a brick building, the range limit on the northern side would be attained immediately or after just a few meters, owing to the insertion loss.

Up to 100 m of the outdoor area can also be supplied through the windows. For this purpose, the base station must be set up on an upper floor (> 3rd floor, that is two levels above ground floor). Low-lying obstructions near the base station, such as, vehicles or a garage (one or two cars) do not, in this case, cause significant interference.

* Reinforced concrete buildings and/or metal facades:
  These have proven to be limiting factors. Penetration into the building is only possible through windows (up to about 2 m into the building in the case of standard size windows). The windows cannot be made from wire-reinforced or metal-plated glass.

  Wave conduction is possible in alleys between buildings as well as along streets. This results in a larger radio area.

3.3.3 Indoor Areas in Buildings in Brick and Light Construction Materials

* Insertion loss values

  In the case of walls of brick or light construction materials, insertion loss values are relatively small so that even dividing walls of up to 30 m can be penetrated.

* Vertical attenuation

  This is dependent on the ceiling type. In this case, reinforced concrete ceilings that offer higher attenuation in particular compared to brick play a decisive role in range evaluation.

  These ceilings are dimensioned based on the purpose of the building, for example,

  – single-family residence

  – apartment building

  – office building

  – theater

  and so the insertion loss a_e also differs accordingly; see Table 4.

Table 4   *Insertion loss (a_e)/range loss in the radio area*

Insertion object	a_e (dB)	Range loss (%)
Brick wall, 10 to 12 cm	2.5	~ 43.5
Brick wall, 24 cm, small windows	4	~ 60
Brick wall, 63 to 70 cm	4.0 to 4.5	~ 60 to 64
Drywall	1.3 to 2.3	~ 26.5 to 41
Gaseous-concrete wall	6.6	~ 78
Glass wall	2	~ 37
Wire-reinforced glass wall	8	~ 84
Reinforced concrete ceiling (residence)	6 to 9	~ 75 to 87
Two reinforced concrete ceilings	26	~ 99.5
Three reinforced concrete ceilings	46	100

NOTE: These values show clearly that propagation within buildings is hindered much less in a horizontal direction than in a vertical direction.
This must be taken into consideration when installing the base station.

3.3.4 Indoor Areas in Reinforced Concrete Buildings with Diverse Interior Layout

Indoor areas in reinforced concrete buildings can give rise to different scenarios, depending on the interior layout.

- **Scenario 1** - Large factory halls (for manufacturing or office space)

   These are either not partitioned (e.g. manufacturing halls) or have mobile partitions reaching half way to the ceiling (office).

   – Propagation conditions

   Favorable in this scenario because intervisibility is more frequent than, for example, in buildings divided into individual offices with no line of sight between the base station and mobile telephones.

- **Scenario 2** - Interior in buildings of brick and light construction materials

   – Propagation conditions

Similar to buildings with brick outer walls.
However, due to industrial sector requirements, the dimensions of reinforced concrete ceilings in these buildings are such that insertion loss values are considerably higher than in brick buildings.

NOTE: The resulting unfavorable vertical wave propagation must be taken into consideration when installing the base station.

• **Scenario 3** - Interior with concrete walls and steel dividing walls

These areas also usually include the heavily steel-reinforced areas of

– stairwells,

– bathroom areas,

– supply shafts, as well as

– elevator shafts.

Table 5 shows several insertion loss values which are relevant to this scenario, along with the corresponding capacity loss data for the radio area.

Table 5   *Insertion loss (a_e)/range loss in the radio area*

Insertion object	a_e (dB)	Range loss (%)
Concrete wall, interior, 10 cm	6	~ 75
Concrete wall, double, 2 x 20 cm	17	~ 97.5
Concrete wall, 25 to 30 cm	9.4 to 16	~ 88 to 97.5
Reinforced concrete ceiling	12 to 14	~ 91 to 96
Two reinforced concrete ceilings	35 to 47	100
Three reinforced concrete ceilings	42 to 53	100
Steel wall with wire-reinforced glass	6.5 to 10	~ 75.5 to 90
Steel walls, extending to ceiling, 3.5 m dist.	31 to 41	100

– Propagation conditions

Horizontal and vertical values are approximately the same. It has been determined that in this type of building, transmission usually takes place along corridors if steel divider walls are installed.

As the relatively high insertion loss values show, individual rooms are increasingly supplied via reflection if multiple metal walls are in the direct path.

Concrete walls cause similar conditions to those described above. Elevator shafts and stairwells must therefore often have their own base station if they are to be included in the HiPath Cordless IP range.

3.4 Determining the Installation Site

3.4.1 Indoors

3.4.1.1 In Buildings of Brick or Light Construction Materials

- Horizontal direction
  A base station must be installed at least every 50 m.

- Central installation in the building
  The general rules must be observed.

- Vertical coverage
  Care must be taken to ensure that no more than two reinforced concrete ceilings are in the direct propagation route between the base station and the area of movement of the handsets.
  Other base stations must then be set up in the radio cells if necessary, based on the concentration of stations or the number of handsets.

Assuming that the distribution of handsets in buildings will be fairly uniform, additional base stations should preferably be installed on the floors above or below the minimum required base stations (see Figure 11).

BS Z

BS Z

BS

3rd floor
Open-plan office

2nd floor

BS

Stair-
well

1st floor

BS

Ground floor

Elev-
ator

BS

Basement

BS ⬛ Minimum required base station

BS Z Possible additional base station, for example, for areas with higher concentration

< 25 m

< 50 m

BS

Stair-
well

BS

Elevator

Floor plan 1st floor
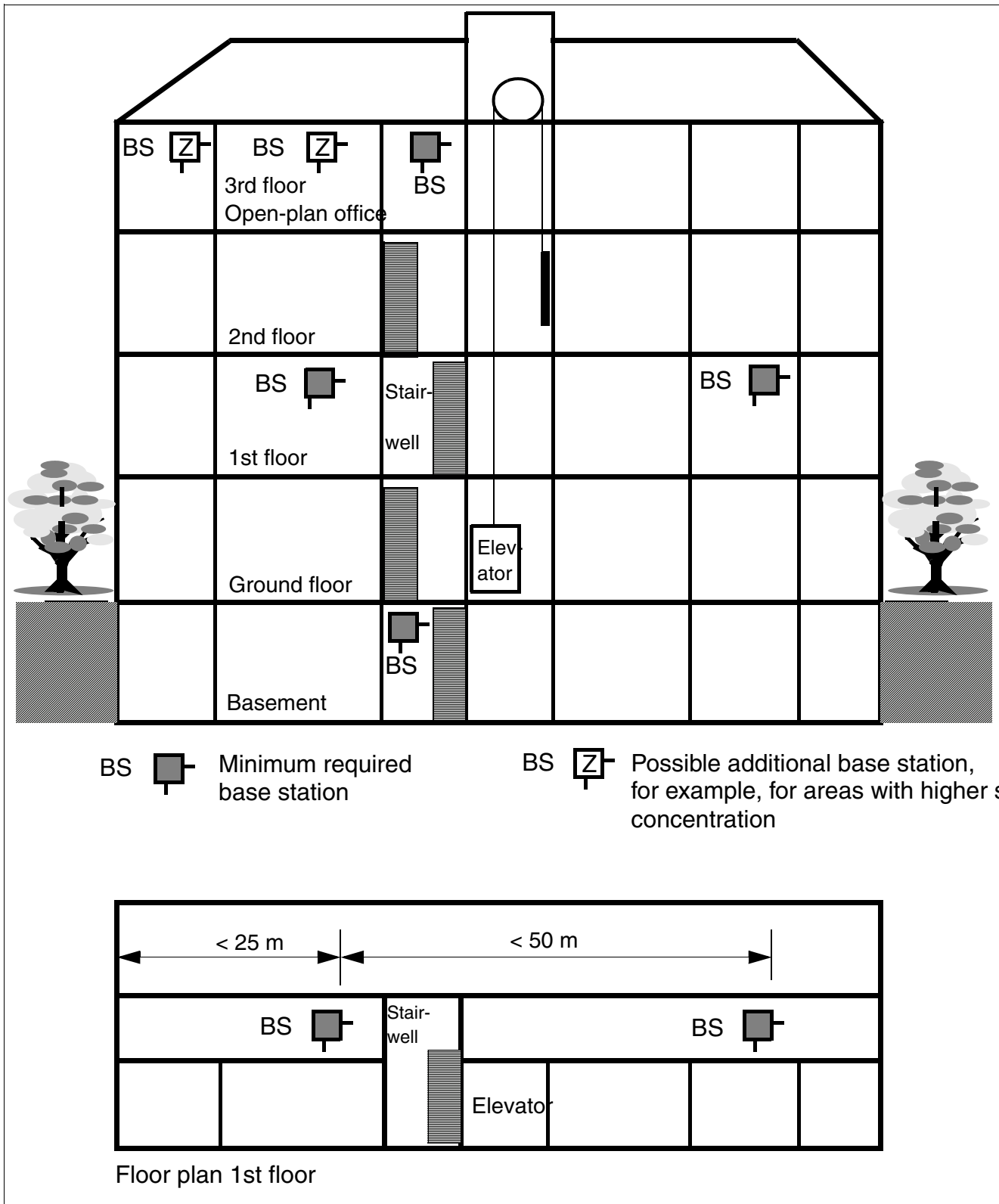
Figure 11   Base station distribution in buildings of brick and light construction materials

3.4.1.2 In Steel/Concrete Buildings

• For interiors of brick or light construction materials (Figure 12)

– Horizontal direction
A base station must be installed at least every 50 m.

– Central installation in the building
The general rules must be observed.

– Vertical coverage
Care must be taken to ensure that not more than one reinforced concrete ceiling is in the direct propagation route between the base station and the area where the mobile telephones are used. Adequate coverage cannot otherwise be guaranteed.

– Stairwells,

– elevator shafts and

– supply shafts

in these buildings usually have strongly-reinforced concrete walls and stairs. Areas such as these, with poor propagation conditions, often require additional base stations.

– If additional base stations are needed because of a large number of mobile telephones, see Figure 12.

| BS ▣ | Minimum required Base station | BS ☑ | Possible additional base station, for example, for areas with higher s concentration |

Floor plan 2nd floor
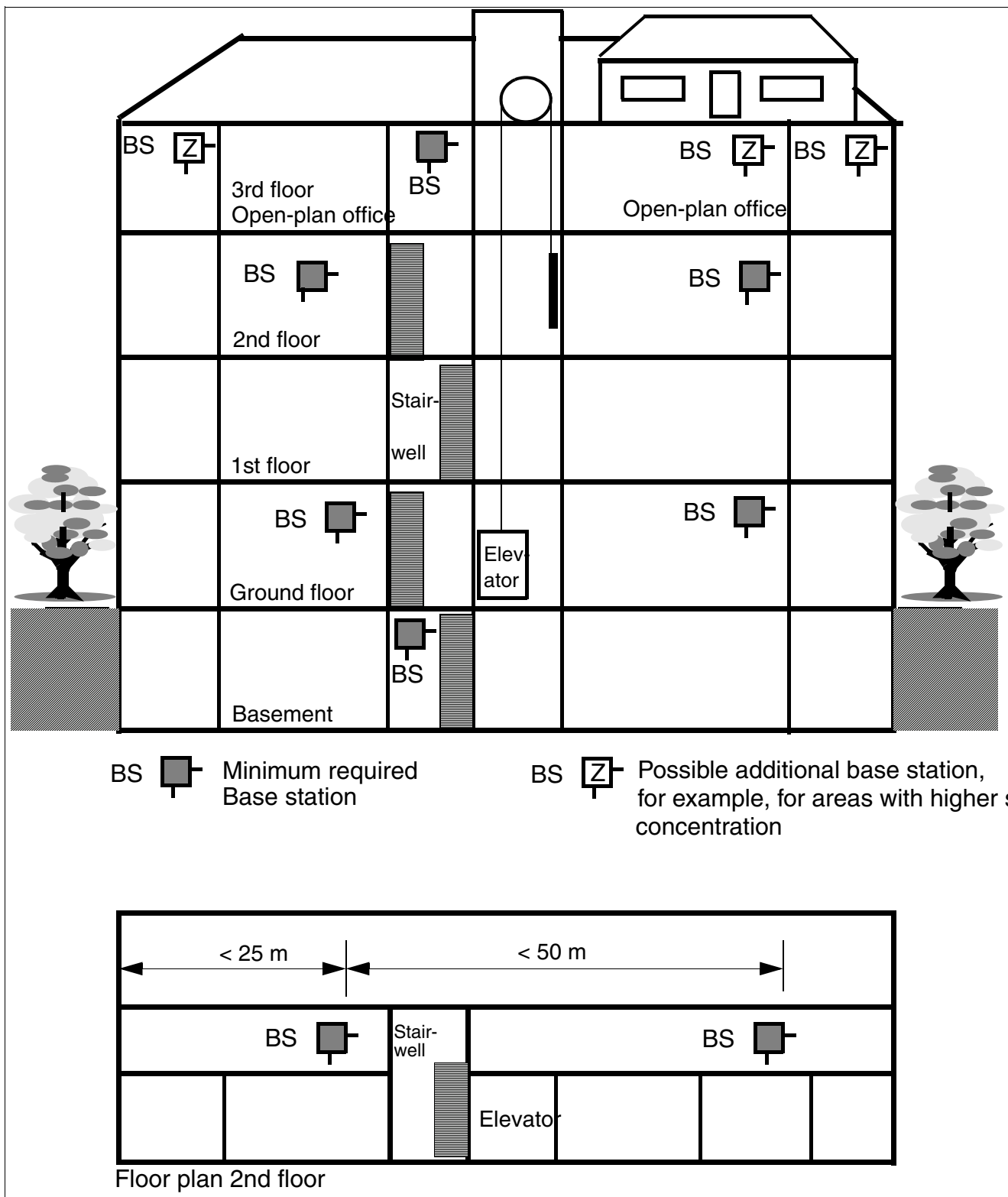
Figure 12   Base station distribution in interiors of brick and light construction materials

- For interiors with concrete and steel dividing walls (Figure 13)

  - Central installation in the building
    The general rules must be observed.

  - Horizontal direction
    Because of the relatively high attenuation of concrete and steel dividing walls, a base station must be installed in these buildings at least every 25 m.

  - Vertical coverage
    Care must be taken to ensure that not more than one reinforced concrete ceiling is in the direct propagation route between the base station and the area where the mobile telephones are used. Adequate coverage cannot otherwise be guaranteed. For

    - stairwells,

    - elevator shafts and

    - supply shafts

    additional base stations are also often necessary.
    In the case of elevators, a base station can be installed in the elevator cabin itself.

  - If additional base stations are needed because of a large number of mobile telephones, see Figure 13.
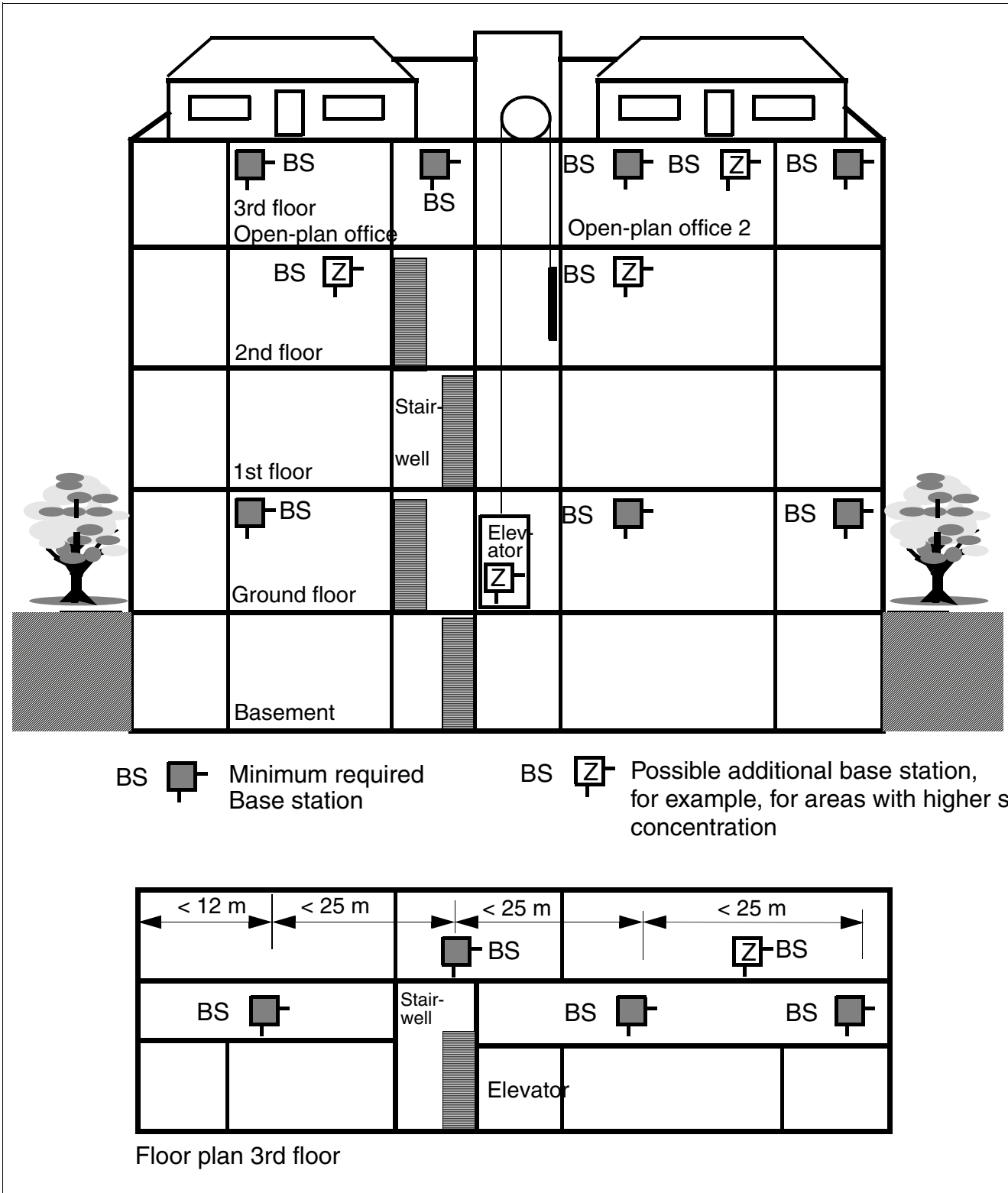
Figure 13   Base station distribution in interiors with concrete and steel dividing walls

3.4.1.3 Factory Halls and Open-Plan Offices

• Within halls or open-plan offices (Figure 12)

Good transmission qualities.

For a hall which is 100 m long, one centrally located base station, suspended freely from the ceiling (mast, plastic chain), may be sufficient.

> ⚠ **CAUTION**
>
> **The base station should not be installed on a reinforced concrete pillar because the pillar creates a partial shadow which means that a clear line of sight no longer exists.**
> **In this case, two base stations must be installed 50 m to 75 m apart.**

In the case of outer walls or interior siding and/or hall ceilings made of metal (or metal-clad), it may be necessary to increase the number of base stations and distribute them in such a way as to virtually exclude radio interference through reflections.

3.4.2 Outdoors

• Base station with outdoor housing (Figure 14)

Only base stations with weather-resistant housing are suitable for radio coverage out of doors, e.g. on factory sites.

– Installation

A base station can be installed on a mast made of wood, plastic or concrete (not metal), on the roof of a building (preferably made of brick or light construction materials) or on the wall of a house.

– The mast used must be stable and wind-resistant.

NOTE: Choose the installation site to allow maximum visibility from the base station to the service area.
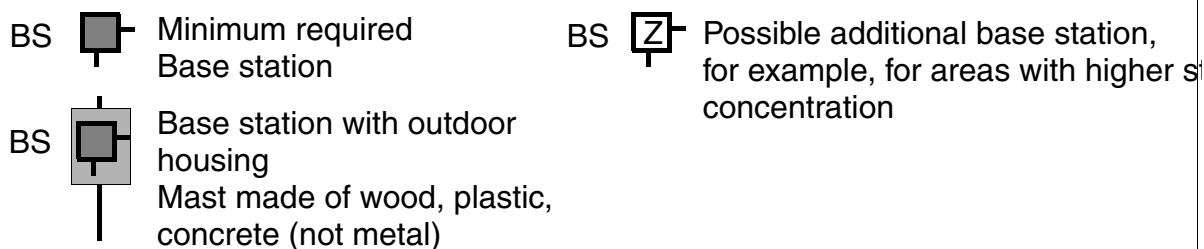
Figure 14   Base station distribution for base stations with housing for outdoor use

Example: Planning an outdoor area (Figure 15)

NOTE: A base station installed in an attic directly beside a dormer window (no metal reinforcement in the window pane) is the alternative to outdoor housing for coverage of the outdoor area.

- Planning

  A site plan, for example, with a scale of 1:300 or 1:1000 is helpful for determining the base station installation site.

  – The customer's preferred radio area should be indicated on the map (subject to customer confirmation).

  – Additional information about the types and heights of buildings is also helpful.

  – Radio coverage can be adequately determined with the aid of the site plan and the information above.

- Site plan, see Figure 15

  This plan depicts a company's grounds with buildings A to G. It includes the type of construction and heights of these buildings.

  – Bird's eye perspective
    It is relatively simple to find the point which offers the best possible view of the grounds without any obstructions.

    Placement around the buildings C, E, F, and G is not feasible since the view from these buildings extends only to a few neighboring buildings.

    The view from buildings A and B is better.

    In the example, the decision was made to place the base station at building B rather than A. Note that the areas between buildings C and E as well as F, G, and A are covered. The radio waves can pass through brick building A, so that an area of about 10 meters beyond will still be covered.

  In practice, coverage can also be assumed for other outdoor areas as waves pass through the windows.

- Reinforced concrete buildings or constructions with metal facades
  act as limiting factors. Areas behind these buildings are quasioptically blocked and must be considered not covered by the radio waves.

- Brick buildings
  can usually be penetrated so that significant parts of them are reached by the radio waves.
  The supply range, however, often stops less than 10 meters beyond these buildings.

Planning a HiPath Cordless IP System

Determining the Installation Site

- Streets
  act as conductors making greater ranges possible along them.
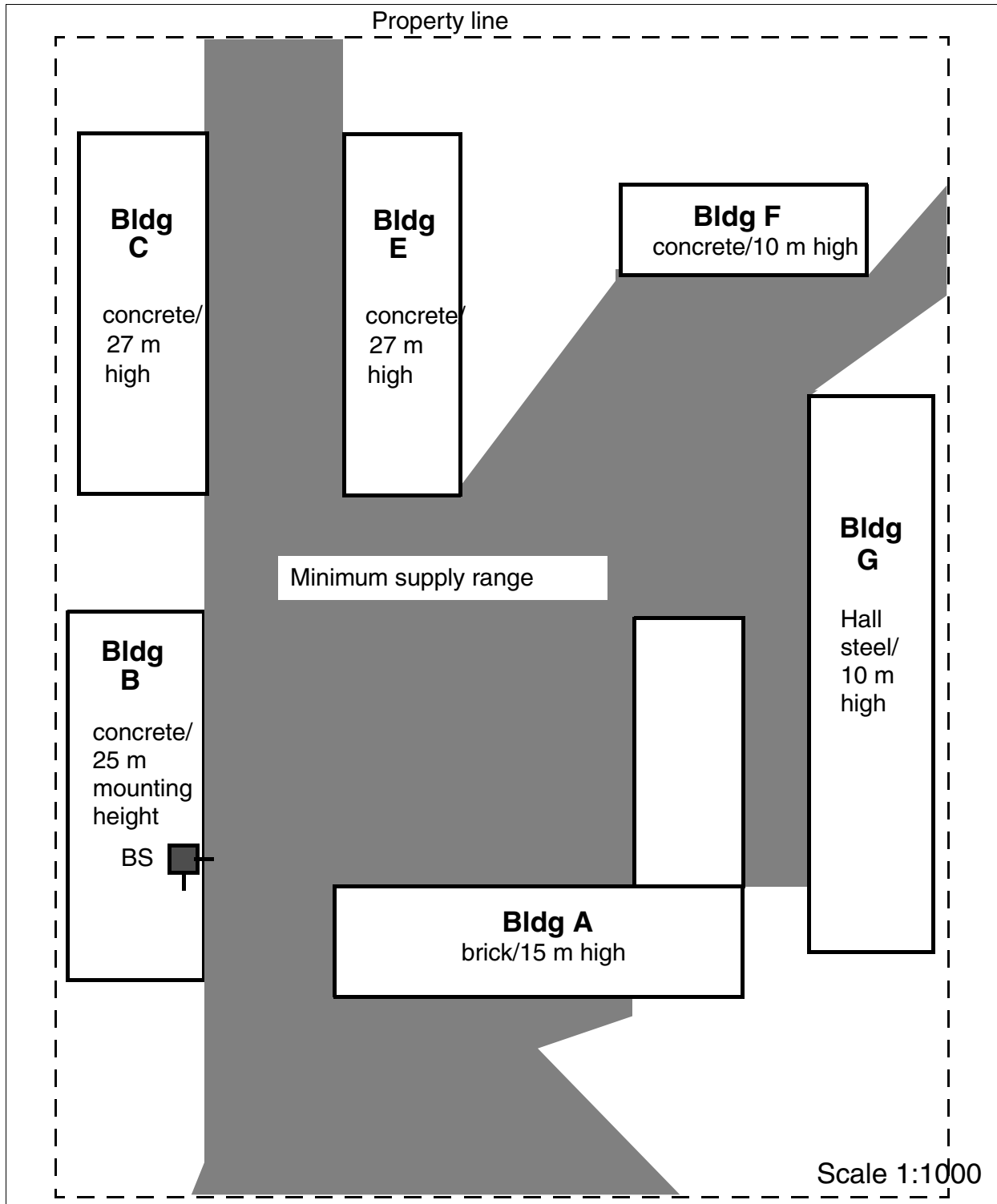
Figure 15   Base station distribution for coverage of an outdoor area

A31003-C1010-S100-4-7620, 09/2011
HiPath Cordless IP, Service Manual

50

3.5 Installing Base Stations

3.5.1 Ethernet Connection Cable

The DECT IP base stations are mounted using Ethernet cables that are terminated with an 8-pin shielded RJ45 connector. The feedthrough in the DECT IP base station's protective cover is 14 mm in diameter. Please take this dimension into account when choosing the RJ45 connector.

The connection cable inserted into the RJ45 jack must be secured additionally with a cable tie to ensure suitable strain relief (see Figure 1)

Installation:

1. First loop the cable tie around the protrusion on the printed circuit board (see Figure 2).
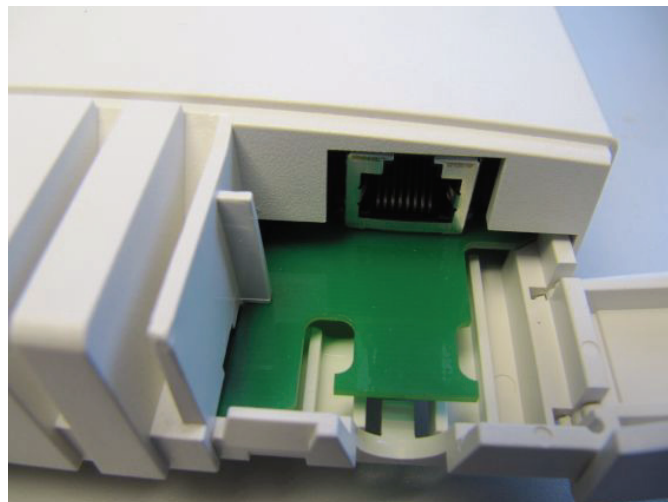
2. Then insert the cable through the loop into the RJ45 jack and tighten the cable tie around the notch on the printed circuited board and the connection cable (see Figure 3).
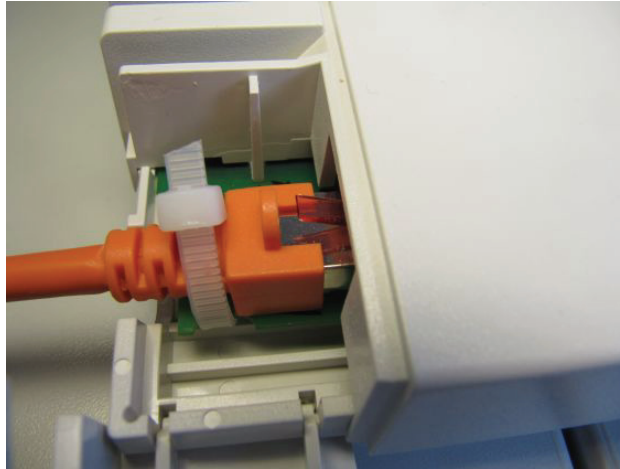
3.5.2 Where Not To Install DECT IP base stations

 CAUTION

Security zones
Areas designated by the customer as security zones, such as, intensive care units in hospitals or areas behind fire doors.

* **Ambient temperature/humidity**

    – Ambient temperature from +0°C to +40°C
      Avoid direct sunlight.

    – In damp places, such as bathrooms, laundry rooms, or in the immediate vicinity of heat sources (for example, heaters).

* **Radio area restriction**

    – In wall recesses or on thick or concrete and metal walls, if the radio supply area is behind them.

    – A base station mounted on a steel or concrete pillar cannot supply the radio area which lies behind the pillar.

* In lowered ceilings of metal (conductive materials, for example, carbon fibres).

* On metal walls
  Only if there is a safety distance of > 10 cm.

- On metal storage shelves
  Only if there is a safety distance of > 3 m.

- **Electromagnetic compatibility (EMC)**

  – The installation site should not be in the immediate vicinity of other electronic equipment, such as, regular (corded) telephones, hi-fi systems or office or microwave equipment. Only if there is a safety distance[1] of > 1 m.

  – Directly beside neon/phosphorous lighting tubes, fire alarms, switchgear cabinets, transformer housings, motor housings.
    Only if there is a safety distance[1] of > 1 m.

  – Directly beside antennas of other communication systems.
    Only if there is a safety distance[1] of > 3 m.

3.5.3 Where Should DECT IP base stations be installed?

- Freely accessible,

  – but near the ceiling (> 0.5 m away from the ceiling).
    (This prevents the base station being blocked by furniture.)

- As centrally as possible in buildings,

  – for example, in corridors or on walls of directly adjacent rooms (in the case of buildings of light construction materials).

- Outdoor areas

  may be part of the coverage area.

NOTE: When planning the installation of base stations in buildings (determining the installation site), architectural plans (scale of about 1:1000) which show the structural type of the building can be very helpful.

  – Near windows facing in the direction of the outdoor area to be covered.

  – Outdoor housing, see Section 3.5.6.

---

1. The safety distance isolates the installation from other equipment, thus improving the electromagnetic compatibility (EMC).

3.5.4 Indoors

3.5.4.1 Wall Mounting

The base station must be freely accessible.

NOTE: When installing a DECT IP base station, the antennas should face downward.

–	Antenna position	Antennas pointing towards open space, in direction of radio area
–	DECT IP Base station mounting position	vertical/180° rotated
–	Mounting	Mounting material not included in scope of supply

– Two wall anchors with 5 mm diameter, two screws with 3.5 mm diameter.

1. Drill two holes (5 mm diameter) 110 mm apart in the wall where the base station is to be mounted. Insert the wall anchors in the hole (see Figure 20).

2. Screw in the screws in such a manner that a clearance of about 4 mm remains between the head of the screw and the mounting wall. Different mounting material may be needed depending on the composition of the mounting wall, for example, wood screws for wooden walls.

   Alternative: You can use the housing feet openings in the base plate of the base station for mounting on wall hooks.

3. Mount the base station on the screw heads or wall hooks.
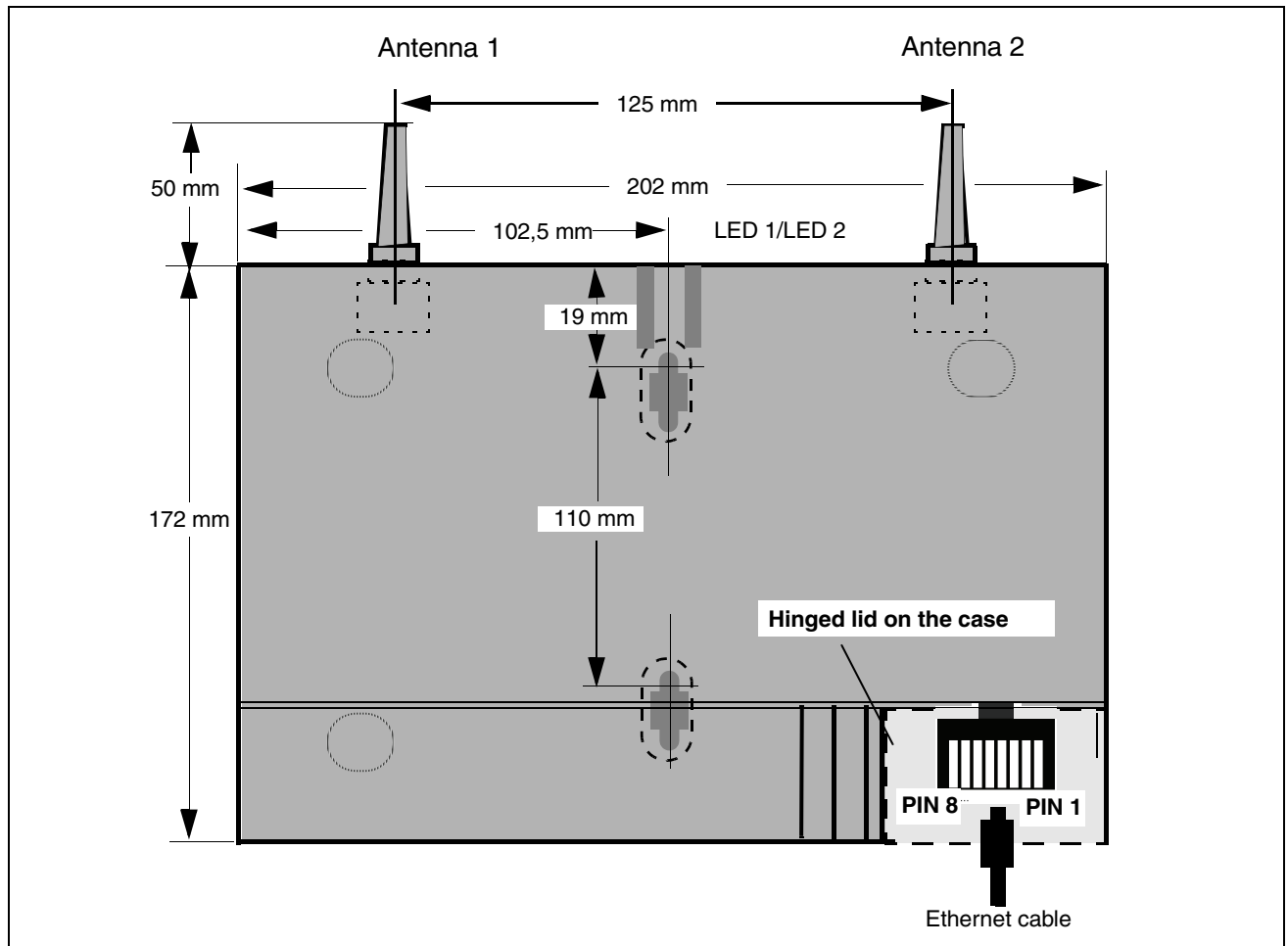
3.5.4.2 Ethernet Socket Allocation in the DECT IP Base Station

PIN	Signal MDI	Signal MDI-X
1	Tx+ (V+)	Rx+ (V-)
2	Tx- (V+)	Rx- (V-)
3	Rx+ (V-)	Tx+ (V+)
4	V+	V+
5	V+	V+
6	Rx- (V-)	Tx- (V+)
7	V-	V-
8	V-	V-

Table 6   *Belegung der Ethernetbuchse*

3.5.5 Tools/Aids

The tools and aids listed below will be required when carrying out the activities described in the following sections. However, they are not included in the delivery scope.

Table 7   Tools/aids

Designation	Application
Crosstip screwdriver size 3	To attach installation plate, sun shield
Crosstip screwdriver size 2	To attach mast blocks/mast installation of outdoor housing
Triangle head screwdriver M 6	To attach and close the housing/outdoors
Aids	
Masonry drill, 8 mm diameter	To drill holes for wall installation, housing/outdoors
Masonry drill, 5 mm diameter	To drill holes for wall installation, housing/indoors

3.5.6 Outdoors

NOTE: The base station contains an overvoltage protector.

- Features of the outdoor housing

  - No special grounding necessary.
    The outdoor housing is made of 100% plastic.

  - Cable feeder entry.

  - Protection against direct sunlight.

  - Base station protection at ambient temperature between -25°C and +40°C (can be operated without heating, +sunlight).

- Figure 16 shows the components of the outdoor housing.

  - The outdoor housing is supplied preinstalled.

  - The necessary installation material is supplied loose.

  - Install the outdoor housing on a mast or on masonry/wood/brick walls.

  - Connect the cable from the communication system (see Section 3.5.4.2).
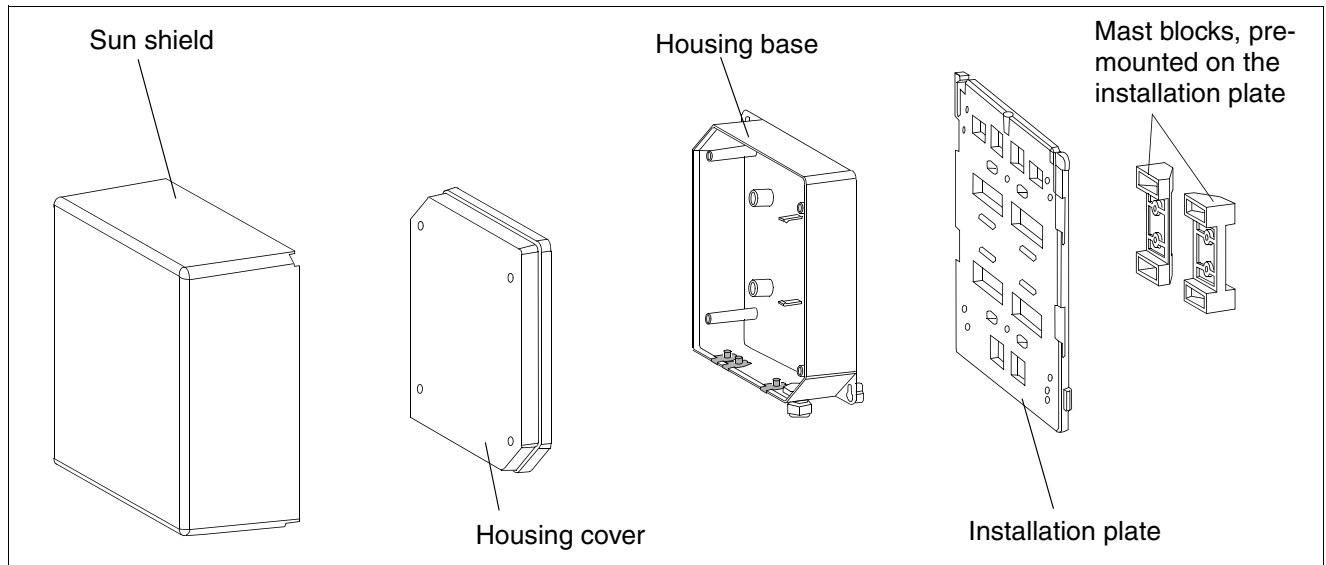
Figure 16 *Components for outdoor installation*

3.5.6.1 Preparatory Tasks

The following tasks must be performed with appropriate tools before installing the outdoor housing:

1. Release the sun shield catches and remove the sun shield.

2. Loosen the special screws that connect the base of the outdoor housing to the mounting plate and remove the outdoor housing.

3. Open the outdoor housing (four M6 triangle head bolts in the cover).

4. Remove the hinged lid to connection plug X1.

5. Install the base station in the recess provided for this purpose making sure it locks into place (listen for the latching noise).
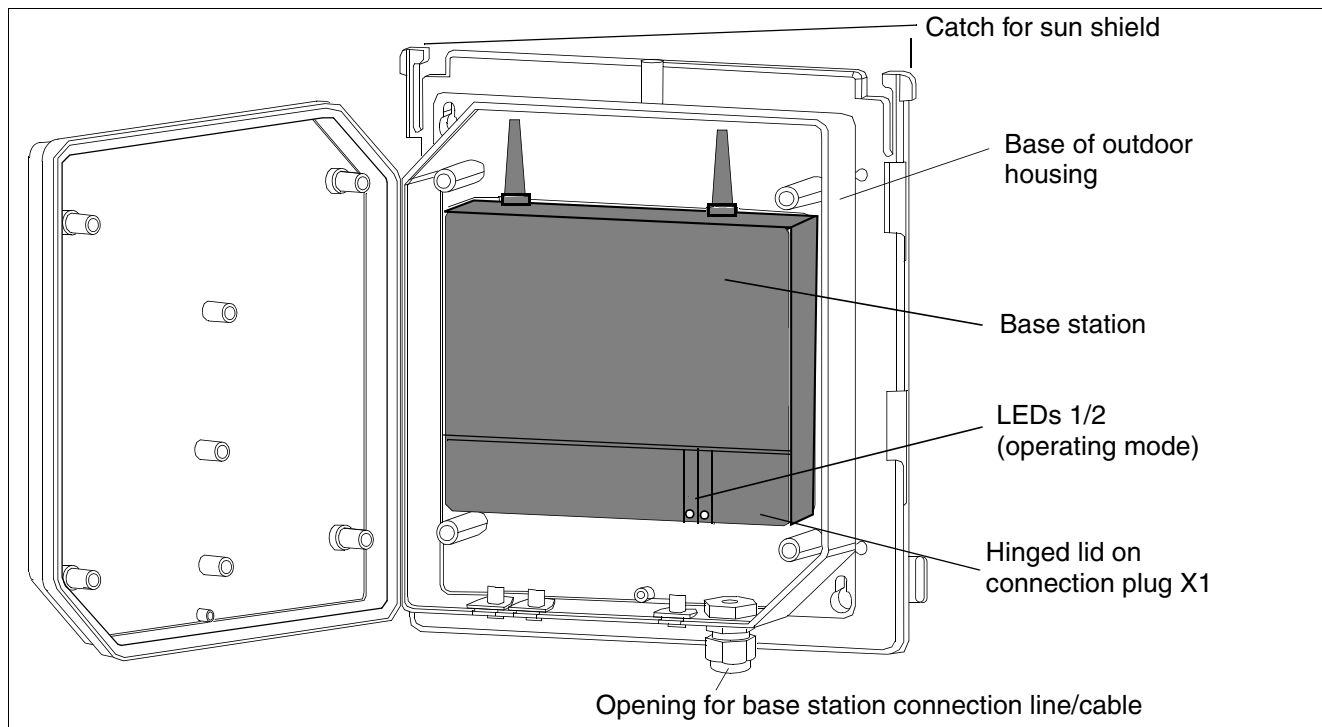
Figure 17   Outdoor housing with base station

3.5.6.2 Mast Installation

Material required (supplied loose): two metal tightening straps.

1. Loosen the mast block fastening screws.

2. Set the distance of the mast blocks to the necessary mast diameter at the required height and tighten the screws.

3. Feed the metal tightening straps through the specially-provided holes in the installation plate, see Figure 18.

4. Attach the base of the outdoor housing to the triangle head bolts on the installation plate.

5. Screw the triangle head bolts tight.

6. If necessary:
    Thread a sealing wire through the lower right fastening hole on the base and the sealing hole on the mounting plate, see Figure 18.
    Seal the wire.

7. Attach the installation plate to the mast at the required height with the metal tightening straps. The mast used must be stable and wind-resistant.

⚠ **CAUTION**

Do not install the base station on steel masts.
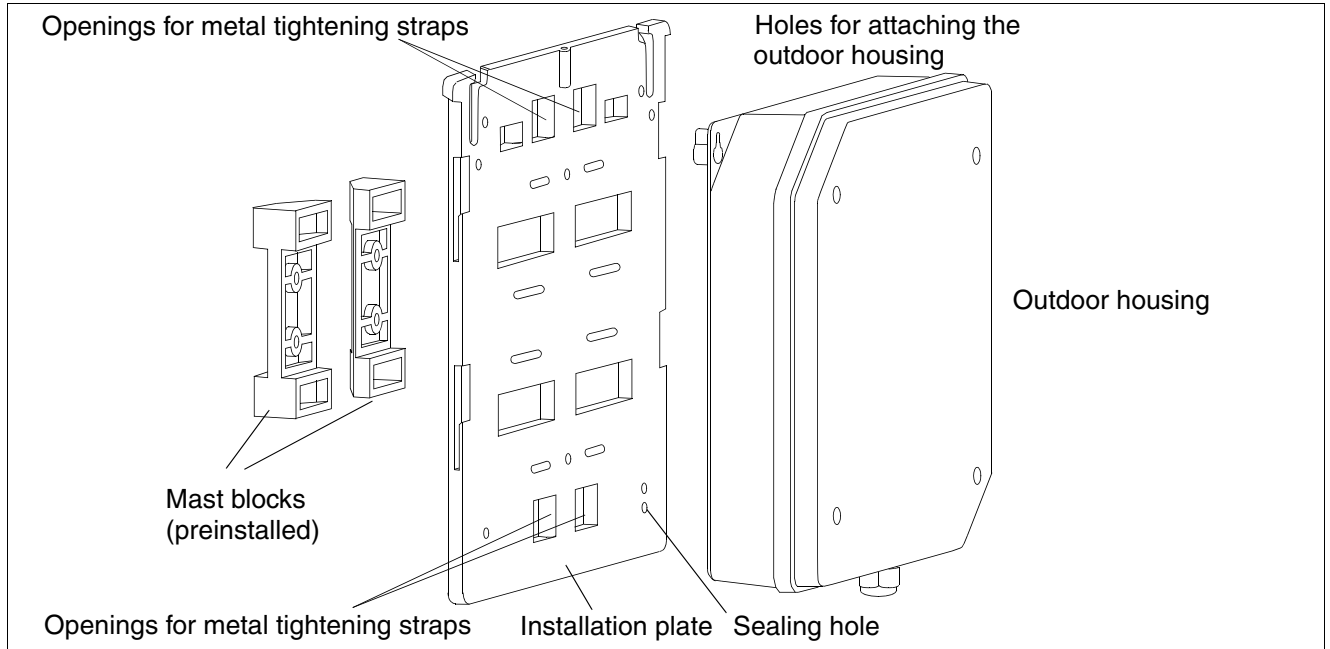
Figure 18   Outdoor housing with mounting plate and mast blocks
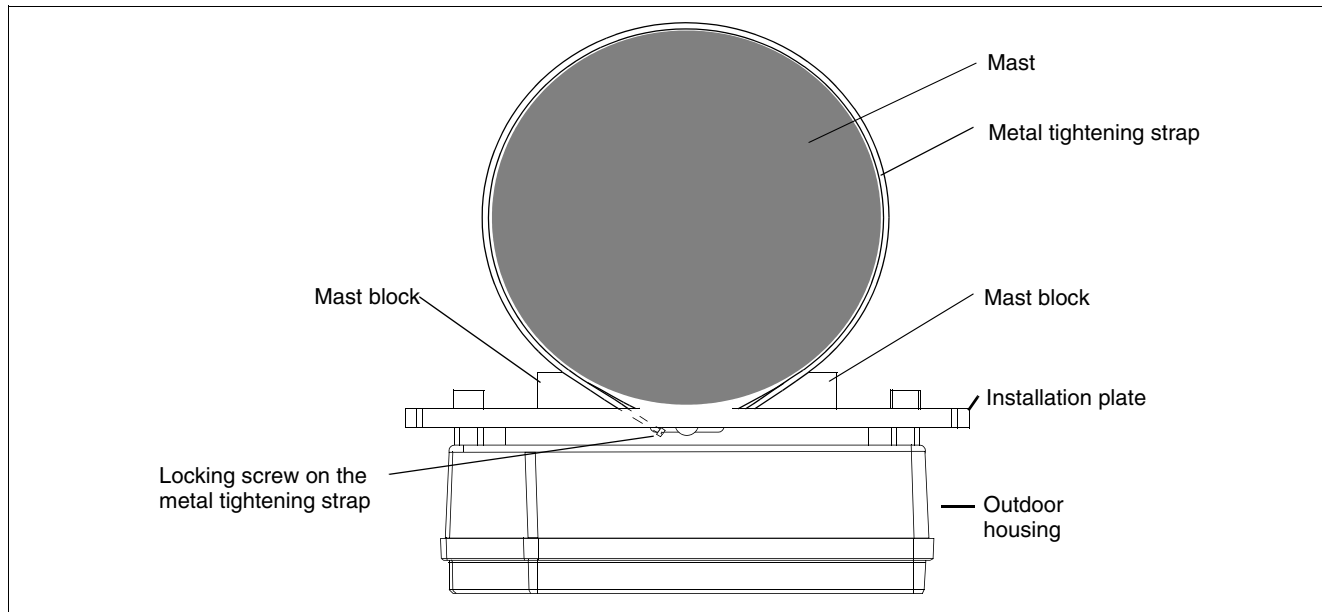
Figure 19   Mast installation – plan view

8. Connect the base station connection cable(s) (see Section 3.5.4.2).

9. Secure the housing cover with the four triangle head bolts.

10. If necessary: lock the sun shield into the spaces on the sides of the installation plate.

3.5.6.3 Wall Installation with Mounting Plate

Material required:

–   Two wall anchors of 8 mm diameter, two screws of 6 mm diameter.

NOTE: Different mounting material may be needed depending on the composition of the mounting wall, for example, wood screws for wooden walls.
In such cases, change/purchase the appropriate mounting material.

1. Drill two holes (8 mm diameter) in the wall where the base station is to be mounted.
    For dimensions, see Figure 20.

    –   Ensure that there is enough room for the mounting plate.

    –   Insert the wall anchors in the holes.

2. Remove the mast blocks from the mounting plate.

3. Attach the mounting plate to the wall with the two screws.

4. Attach the base plate of the outdoor housing to the triangle head bolts on the mounting plate.

5. Screw the triangle head bolts tight.

6. If necessary:
    Thread a sealing wire through the lower right fastening hole on the base and the sealing hole on the installation plate and seal it (see Figure 18).

7. Connect the base station connection cable(s) (see Section 3.5.4.2).

8. Secure the housing cover with the four triangle head bolts.

9. If necessary: lock the sun shield into the spaces on the sides of the installation plate.

3.5.6.4 Wall Mounting Without Mounting Plate

Material required: two wall anchors of 8 mm diameter

1. Drill two holes (8 mm diameter) in the wall where the base station is to be mounted.
    For dimensions, see Figure 20. Insert the wall anchors in the holes.

2. Screw the two triangle head bolts through the mounting plate and into the wall anchor so that a clearance of about 12 mm remains between the screw head and the mounting wall.

3. Hang the base plate of the outdoor housing into the screws by its tabs (upper left and lower right) and tighten the screws.

4. Connect the base station connection cable(s) (see Section 3.5.4.2).

5. Secure the housing cover with the four triangle head bolts.

NOTE: The sun shield cannot be mounted without the mounting plate.
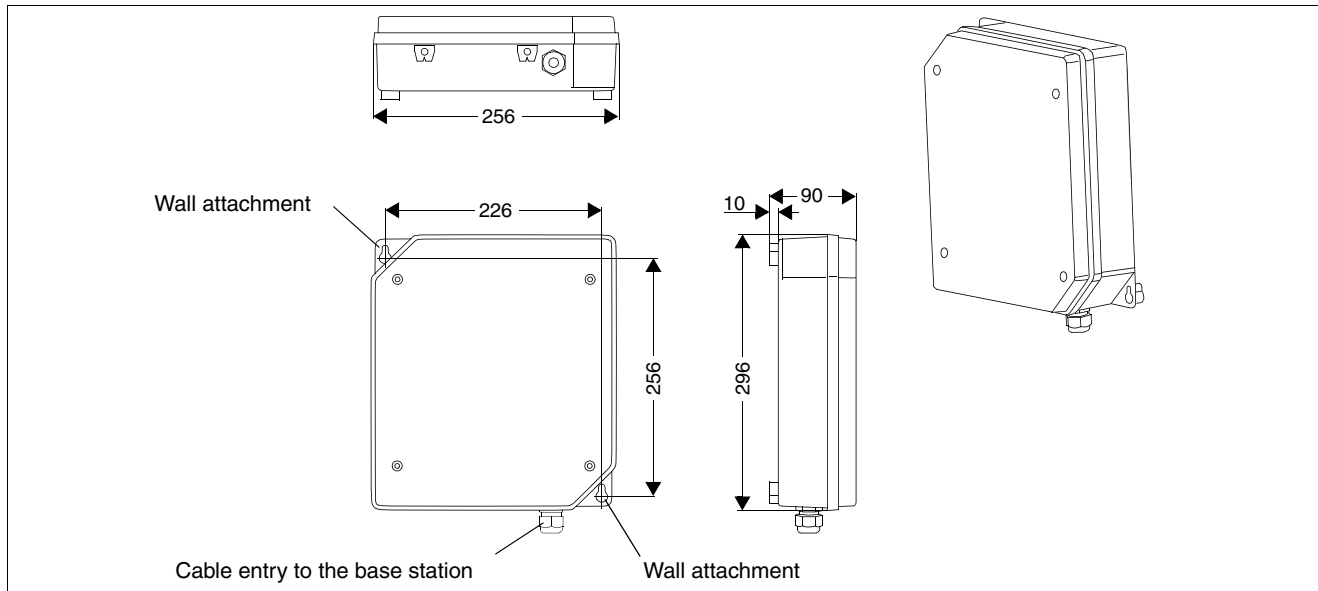
Figure 20   *Wall mounting without mounting plate*

4 Putting Into Service

You can only put your HiPath Cordless IP system into operation after the

- planning,

- coverage,

- installation and cabling,

- installing the communication server and if necessary, the HiPath Cordless IP server.

requirements have been fulfilled. The installation of the HiPath Cordless IP system now starts.

4.1 Preparation

1. DECT handsets are charged.

2. DECT system ID is available.

3. LAN suitability for VoIP services is analyzed (refer to Section 3.3).

4. Administration access is available for the HiPath Cordless IP server software's Web-Based Management application.

5. Information is available on subscribers, stations numbers, names.

6. There is a sufficiently large number of IP addresses available for use for the HiPath Cordless IP server software and the DECT IP base stations.

7. The IP address of the communication server, the DHCP server and the DNS server is determined.

8. The customer data available is backed up.

Optional if these services are to be used:

9. The PoE injectors are available.

4.2 Entering the DECT System Number (DECT ARI)

The DECT system number consists of eight hexadecimal characters and is unique worldwide for each DECT system.

The DECT system number is the number used to identify the individual DECT systems and therefore to identify the radio signals (radio range). This permits the synchronization of mobile telephones logged on to the system.

The DECT system number consists of:

• E/ARC (Access Right Code, 4-bit (first digit is always 1)

• EIC (Equipment Installers Code, 16-bit),

• FPN (Fixed Part Number, 8-bit), and

• FPS (Fixed Part Subnumber, 4-bit).

When installing the system for the first time, you must apply for the DECT system number which then applies to the entire HiPath Cordless IP server software (even in the event of service).

The DECT system number is stored in the HiPath Cordless IP server software database.

This system number should be stored safely (loss).

4.3 Overview IP adresses
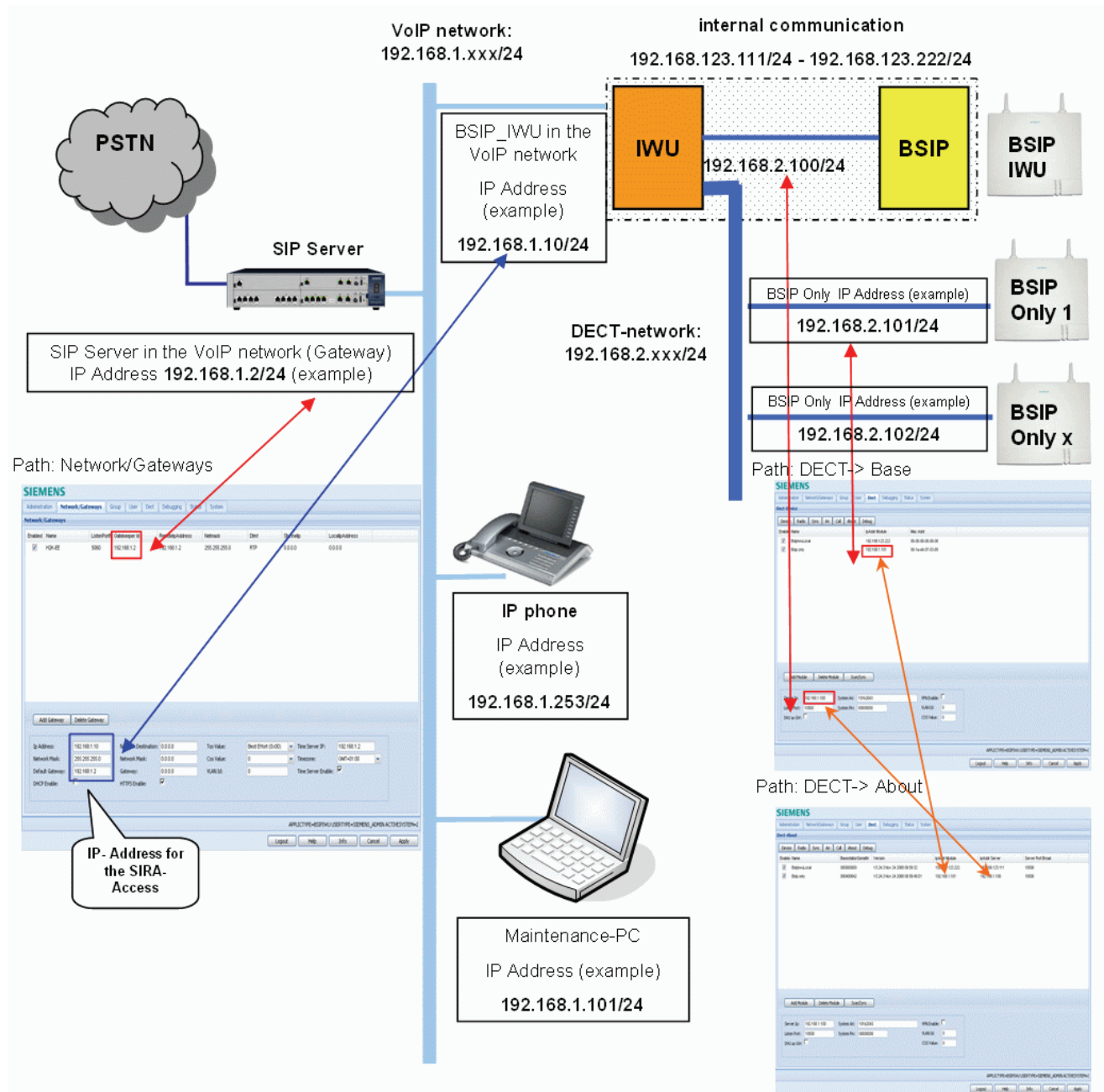
5 Installation and Administration

5.1 Introduction

5.1.1 Scope

This document describes both platforms of the HiPath Cordless IP System:

- HPCIP - Small Solution: The HiPath Cordless IP Server Software (HPCIP-IWU*) is running on a BSIP (BSIP-IWU).

- HPCIP - Server Solution: The HiPath Cordless IP Server Software (HPCIP-IWU) is running on a dedicated Server "FSC Tx150 S7" (Server-IWU).

Unless otherwise noted, the instructions in this document refer to both platforms.
  * IWU = InterWorking Unit

5.1.2 Terminology

The terms "Voip gateway" and "PBX" are used as a synonym for the supported Siemens communication servers OpenScape Office MX (OSO MX), HiPath 3000, HiPath 4000 and OpenScape Voice (OSV).

The term **BSIP-Only** is used as a synonym for a BSIP which is **NOT running** the **HiPath Cordless IP Server Software**.

Therefore the term **BSIP-IWU** is used as a synonym for a BSIP which **IS running** the **HiPath Cordless IP Server Software**.

5.1.3 Network Concept

The IP network concept of the HiPath Cordless IP solution System is designed for the separation into three logical networks:

1. **VoIP (Infrastructure) network**

   Here the existing infrastructure components (default Gateways, DHCP servers, Time server, ...), the **PBX** (the VoIP Gateway) and the BSIP running the HiPath Cordless IP Server Software (the Interworking Unit [IWU] between VoIP and DECT) are located. This network is used for the connection of the IWU to the IP and VoIP infrastructure of the company LAN.

   The factory-default network address is 192.168.2.0 with a netmask of 255.255.255.0.

The preconfigured IP address of the IWU in this network is 192.168.2.1.

2. **DECT network**

   Here all BSIP-Only Base Stations and the BSIP-IWU or the server running the HiPath Cordless IP Server Software (IWU) are located. This network is solely used for the communication between the IWU (BSIP-IWU or Server-IWU) and the BSIP-Only.

   The factory default network address is 192.168.1.0 with a netmask of 255.255.255.0.

   The preconfigured network address of the BSIP-IWU inside the DECT network is 192.168.1.1 with a netmask of 255.255.255.0.

   The IP addresses for this networks segment may be - apart from the exceptions in the next chapter - configured freely.

3. **BSIP internal networks**

   For internal communication between the different hardware components of the BSIP there are two further networks configured.

   • **Important:** These addresses are fixed and cannot be changed. Keep in mind, that these addresses may not be used for the VoIP network and the DECT network. Furthermore no other components which are accessing the IWU or BSIP-Only may use one of these addresses.

   192.168.123.x :
   Network between the BSIP Local DECT module (.222) and the BSIP-IWU (.111).

   169.254.222.x :
   Network between the two main processors CSP (.1) and 192.168.123.x MSP (.2) for internal communication.

   • **Important:** All BSIP devices must be located inside the same network segment and therefore **MUST NOT** be separated by layer 3 routing devices. Only Layer 2 switches are supported between the BSIPs.

5.1.3.1 Overview of reserved networks

Host IPs 192.168.1.1/24 and 192.168.2.1/24 are used for factory defaults of BSIP-Only and BSIP-IWU

IP network 192.168.123.0/24 for internal communication between CSP and DECT Basebandcontroller (BBC).

IP network 169.254.222.0/24 for internal communication between CSP and MSP.

5.1.4 Synchronization over air concept

In contrast to a line based synchronization mechanisms (or a network based one), synchronization via air requires special requirements.

Synchronization signal

Both synchronization partners are syncing over air. This means that the synchronization signal received by the synchronization client from the synchronization master has to have specific minimum signal strength. The theoretical minimum signal strength for the synchronization signal is -85 dB. The minimum aspired signal strength for the synchronization signal is -75 dB

Synchronization topology

For the operation of several synchronized Base Stations several topological approaches are possible.

1. Star based synchronization topology

This topology uses just one Base station of the whole system as a synchronization Master (Sync Master). All other Base stations which take part at synchronization are working as synchronization Slaves (Sync Slave) and receive their synchronization signal from the only Sync Master.

2. Chain based synchronization topology

This topology uses just one Base station of the whole system as a synchronization Master (Sync Master). All Base Stations are arranged - in terms of topology - in a chain.

The second Base Station receives its synchronization signal from the Sync Master and additionally provides the synchronization signal for the next Base Station in the chain that is this it serves as well as **Sync Slave** AND as **Sync Master**.

The second BSIP synchronizes to the first BSIP, the third BSIP synchronizes to the second BSIP, the fourth synchronizes to the third BSIP and so on.

Both topologies may be mixed to achieve large-scale radio coverage.

Important Notes:

• The distance between a "Sync Slave" to the topmost "Sync Master" must not be more than 5 hops (including the Master Base and the last Slave Base) else the "synchronization slip" will be too large.

• A resynchronization process will be initiated automatically if no call (at the belonging Base Station) is active.

• Avoid using a chain topology which is physically arranged as a circle. In such a scenario, the drift between the first and the last base station may be too large to ensure proper handover between these two Base Stations.

- In contrast to a line or Ethernet based synchronization the synchronization signals is transmitted over air. To achieve efficient signal strength of the synchronization signal the "radio distance" between two synchronized base Stations is crucial. This fact has to be considered adequately during the radio site survey.

- If a BSIP loses synchronization it tries to resynchronize to its configured synchronization base station. This process can not start until the last call at this base station is released and no other calls (at the belonging base station) are active.

5.1.5 Synchronization via Ethernet (acc. IEEE 1588)

In contrast to a air based synchronization mechanisms, synchronization via Ethernet (acc. IEEE1588, PTP Precious Time Protocol) requires less configuration.

On the other hand, great demands are made on the Ethernet characteristics like symmetry, packet loss, delay, jitter (variance of delay), … Therefore special requirements regarding the Ethernet components (especially the Ethernet switches used) have to be considered. Exceeding of limits (especially of jitter) will lead to loss of synchronization, which will finally lead to a resynchronization process. During this process the belonging Base Stations are unable to establish telephony connections.

Synchronization topology

The Synchronization according Ethernet solely uses a star shaped topology. Maximally one Base Station serves a Synchronization Master (Sync Master), all other Base Station which participate at the synchronization serve as Synchronization Slaves (Sync Slave).

Resynchronization

The DECT functionality of all BSIP, which are configured as IEEE1588 Sync Slaves, depend on the availability of the IEEE1588 Sync Master. If the Sync Master is not functional (e. g not Online due to Ethernet problems …), the DECT functionality of all IEEE1588 sync slave BSIP will go down. During this time no telephony is possible.

General requirements on the Ethernet system

A maximum number of three cascaded Ethernet switches are supported between the Sync Master (SM) and a Sync Slave (SS) BSIP.

Only premium class switches, which fulfill the requirements regarding Ethernet synchronization according IEEE1588, are supported. A list of supported switches is documented in the sales information of the HPCIP system.

Usage of VLAN at the BSIP-IWU for Infrastructure and DECT network is mandatory. All participating switches have to be configured in a way that the VLAN of the DECT network has to be assigned the highest priority.

Further details regarding Ethernet Synchronization according IEEE1588 may be found in chapter 5.4.1.3, "Ethernet Synchronization (acc. IEEE1588)".

5.1.6 WBM related issues

5.1.6.1 Supported Web Browser

The following web browsers are supported:

- Mozilla Firefox Versions 2.x, 3.0.x, 3.5.x and 3.6.x

- Microsoft Internet Explorer Version 6.x, 7.x and 8.x

For details refer to chapter 5.7.1, "Configuration hints for Web Browser" as well as the release notes.

5.1.6.2 General WBM issues

- Don't use special characters inside the objects for WBM. Supported characters are
0-9, a-z, A-Z, "-" "_". Other characters (especially "[", "]", ASC 0x00 - ASC 0x1F) may lead to problems.

- Don't configure names for objects with more than 20 Characters.

- Configuration and firmware files MUST NOT include spaces in their filenames

- Do not use multiple WBM session to different BSIPs at a single browser session. This may influence the behaviour of the WBM sessions.

5.1.6.3 Simultaneous WBM sessions

If you login onto the same WBM session on which another user is logged on, you are informed about that by a message box.
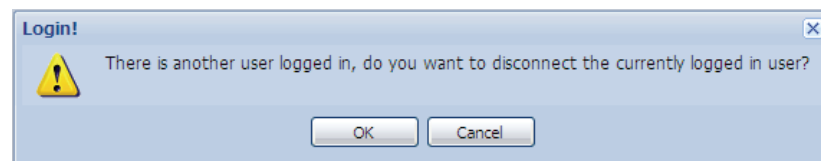
[OK] will logout the currently connected user.

[Cancel] Go back to the Login dialog.

5.1.6.4 Marking changed values

Changed values are marked with a red triangle at the top left corner of the corresponding field. But you have to leave the current field for changes to come in effect (via TAB key or mouse).

Marker for changed values (red triangle):

DisplayName	Comment
default 1	741

Please keep in mind that changes are not in effect immediately. You have to

• apply the changes with the [Apply] button and for some changes you have to

• restart the services or for some changes

• reboot the BSIP

Information which actions have to be taken to take the changes into effect will be described in the appropriate chapters.

5.1.6.5 Sorting of Tables

All tables may be sorted (Ascending or Descending) by either double-clicking the column header or by left clicking of the arrow in the right area of the column header.

User	Msn	▼ Voip states	Ras ch	Call states	L
761	761	Sort Ascending		Connected out	1
762	762	Sort Descending		Connected in	1
763	763	Ras up	1	Located on	1
00A7C3(	999	Ras down	0	Located on	1

Modules1 Modules2 CallsDect RSSI

• **Hint:** Sort properties are not stored. After a change of pages the original sort order is restored.

5.1.6.6 Drag and Drop Support

Besides the standard mechanism of sorting user entries by clicking the column headers individual user entries may be reordered using a drag and drop mechanism.
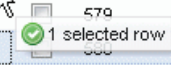
1. Select the user entry that should be moved by pressing the left mouse button.

8	☐	576	DISP-576	SL1 Dect-Test#46 (576 Deutsch	HOOME
9	☐	577	DISP-577	SL1 Dect-Test#47 (577 Deutsch	HOOME
10	☐	578	DISP-578	S4 Dect-Test#48 (578 ⊦ Deutsch	HOOME
12	☐	579	DISP-579	S3 Dect-Test#49 (579 ⊦ Deutsch	HOOME
11	☐	580	DISP-580	S4 Dect-Test#50 (580 ⊦ Deutsch	HOOME

⊘ 1 selected row

2. Drag the selected entry to the new designated position.

8	☐	576	DISP-576	SL1 Dect-Test#46 (576 Deutsch	HOOME
9	☐	577	DISP-577	SL1 Dect-Test#47 (577 Deutsch	HOOME
10	☐	578	DISP-578	S4 Dect-Test#48 (578 ⊦ Deutsch	HOOME
12	☐	579	DISP-579	S3 Dect-Test#49 (579 ⊦ Deutsch	HOOME
11	☐	580	DISP-580	S4 Dect-Test#50 (580 ⊦ Deutsch	HOOME

⊙ 1 selected row

- **Hints:**
  The entry will be added above the selected entry if the selected row if the drag direction is upward.
  The entry will be added below the selected entry if the selected row if the drag direction is downward.

3. Drop the dragged entry by releasing the left mouse button.

8	☐	576	DISP-576	SL1 Dect-Test#46 (576 Deutsch	HOOME
9	☐	577	DISP-577	SL1 Dect-Test#47 (577 Deutsch	HOOME
11	☐	580	DISP-580	S4 Dect-Test#50 (580 ⊦ Deutsch	HOOME
10	☐	578	DISP-578	S4 Dect-Test#48 (578 ⊦ Deutsch	HOOME
12	☐	579	DISP-579	S3 Dect-Test#49 (579 ⊦ Deutsch	HOOME

4. Save your changes by clicking the [Apply] button.

5.1.6.7 Configuration Changes according Service State

While system services are running, the content of the tables below "Network/ Gateways", "Group", "User" and "Dect" are read-only. Therefore you have to stop the system services (Offline mode) to edit these values.

To enable the configuration of User settings during running system services, there is a special functionality ([Edit user]) available. You may add, delete or modify existing user entries.

To modify existing user entries, select a user row and click on [Edit user]. Now the entries in the table row are editable. Changes for the selected user are locked until the changes are applied using the [Apply] button or are reverted using the [CANCEL] button.

Please keep in mind, if deleting a user entry the DECT registration is NOT being removed. Therefore the entry for the handset will be added later as an auto entry user.

If a user should be deleted during an active call, the object will NOT be deleted. A message box will inform about this.

5.1.7 Phone related issues

5.1.7.1 Date / time for phone idle display

The handset displays the local system time in its idle display.

The activation of date / time at the phone idle display is initiated by an outgoing or incoming call (but no active connection is needed therefore).

If the user changed the LocalTime at the handset, the time will be overwritten with SystemTime after the next incoming or outgoing call.

• **Hint**: There is neither an activation of the current date / time due to a Power cycle of the handset nor to a roaming process.

5.1.7.2 Service Menu

If the handset is in one of the service menus (e.g. Lall List) the menu will be automatically closed by an incoming call and the call is signaled at the handset.

5.1.8 Partition concept of BSIP

To guarantee a functional BSIP at any time, two bootable systems are implemented at the BSIP.

A **current system** and the **fallback system**. Therefore the BSIP has two different systems partitions:
System 1 and System 2.

Both system partitions can hold their **own configuration** (although it is copied from one partition to the other during a firmware update).

Both partitions store their application mode (BSIP-Only or BSIP-IWU)

A factory reset is always applied to the **current system** partition. It does **not** affect the settings of the other partition.

- **Hint**: Similar to the BSIP-IWU, the Server-IWU contains the same partition concept as described above.

5.1.9 Factory reset of BSIP

A Factory Reset (resetting the BSIP to its default configuration) may be performed either by

- a local login at the WBM of a BSIP-Only using the Factory Reset button or

- a special "power sequencing" cycle (e.g. if the BSIP WBM is not accessible) using the ethernet cable at the BSIP.

Both methods are resetting the active partition of a BSIP to its factory default configuration.

The factory reset by "power sequencing" is applied by the following process:

1. Power on the board by plugging the ethernet cable (see note)

2. Wait 5s (3s < wait < 7s)

3. Power off the board by unplugging the ethernet cable

4. Repeat steps 1. - 3. three (3) times

5. Boot BSIP to OS

The successful factory reset is indicated by fast red flashing of both LEDs.

- **Note:** If you provide power to the board by connecting the ethernet cable using a PoE Switch power may NOT provided immediately. Due to the stages of powering up a PoE link defined in 802.3af it may take up to some seconds until the power is delivered from the switch to the PoE port. Take a look at the LEDs or the switch status LEDs to see at which point the power is available.

After this procedure, the default configuration parameters will be set.

The default application mode after a reset is BSIP-Only mode.

- **Hint**: The factory reset is applied to the currently active partition. It does not affect the settings of the other partition. But both operation mode settings (BSIP-Only and BSIP-IWU) of the active partitions are resetted

Setting	Value
Operation mode:	BSIP-Only
IP address of VoIP network	192.168.1.1
Access mode	http
User Siemens	Username: "Siemens", password "1q21q2"
User SiemensAdmin	Username: "SiemensAdmin", password "1q21q2"

Setting	Value
Operation mode:	BSIP-IWU
IP address of VoIP network	192.168.2.1
Access mode	http
User Siemens	Username: "Siemens", password "1q21q2"
User SiemensAdmin	Username: "SiemensAdmin", password "1q21q2"

5.1.10 Release Notes

Check the release notes of the belonging version of the firmware for restrictions and special considerations.

5.2 Quick Start

The quick start chapter describes the initial operation of the HiPath Cordless IP System V1R3 for a first functional test including the necessary configuration.

In general the configuration steps for both HPCIP platforms (HPCIP - Small Solution and HPCIP - Server Solution) differ mainly in the initial configuration of the IWU. Therefore only these steps are documented separately.

The "Quick Start" assumes the availabilty of

- two BSIP or one HPCIP-Server and two BSIP,

- a functional **PoE network switch**, (alternatively a switch and **Power injectors**) and CAT.5 cables

- **a Maintenance PC** (Windows XP based) with administration account and

- a supported PBX (e.g. OSO MX).

Please read the corresponding chapter in the detailed manual parts if you need further information regarding any step of the "Quick Start".

The following conditions apply:

- For the quick start it is assumed that no VLAN functionality is needed

- No special DECT functionality is configured (Antenna diversity,...).

5.2.1 Quick start overview

1. Prepare and connect hardware

2. Configure BSIP/Server for IWU mode

3. Configuration of VoIP (Infrastructure) Network at IWU

4. Configuration of DECT Network at IWU

5. Configuration of users at the IWU

6. Configuration of users at the PBX

7. Start system services and register handsets at the IWU

8. Attach and configure further BSIP-Only to the system

5.2.2 Example Configuration

Several settings are needed for configuring a HPCIP system. Inside this quick start, following settings are used:

Configuration Option	Value
Page Network/Gateways	
Network/Gateway: Server IP Address:	192.168.100.1
Network/Gateway: Server IP Netmask:	255.255.255.0
Network/Gateway: Default Gateway:	192.168.100.83
Network/Gateway: NTP Server (Time Server):	192.168.201.94
Gateway (PBX) - Name:	OpenScape Office MX 3bx
Gateway (PBX) - IP Address:	192.168.201.94
Gateway (PBX) - Netmask:	255.255.255.0
Page DECT	
DECT: Server IP Address:	192.168.10.1
DECT: Server IP Netmask:	255.255.255.0
DECT: ARI:	101b2ff5
DECT: PIN:	87654321
Page User	
User No. 1: MSN/DisplayName/AuthName/Password	761/761/761/1234
User No. 2: MSN/DisplayName/AuthName/Password	762/762/762/2345
User No. 3: MSN/DisplayName/AuthName/Password	763/763/763/3456

5.2.3 Prepare and connect Hardware

5.2.3.1 HPCIP - BSIP (Small Solution)

Attach the first BSIP to a PoE port of the network switch or via a Power injector to a standard port of the network switch. Wait about 2 minutes until the LED states of the BSIP change to permanently green and red.

Meanwhile you may connect the maintenance PC to a switch port via a ethernet cable.

- **Hint**: The BSIP must reside inside the same layer 2 network segment. The devices MUST NOT be separated by layer 3 Routing devices. Only separation via Layer 2 switches is supported.

5.2.3.2 HPCIP - Server (Server Solution)

Connect the HPCIP-Server (FSC Tx150 S7) to mains, the necessary peripheral components (monitor and keyboard) and connect the network port using an Ethernet cable with a Standard or PoE-Port of a network switch.

Boot the Server with the installation CD of the HPCIP Server Software. Install and configure according the appropriate instructions (which are not part of this documentation).

Remove the CD and reboot the server again with the newly installed HPCIP Server software.

*   **Hint:** Possibly an update to the latest released HPCIP Server Version (V1R3) should be accomplished. Optionally update twice so that the active system partition is Partition 2. (Since all newly attached BSIP also come up with system partition 2 as the active partition).

5.2.4 Configure BSIP/Server for IWU mode

5.2.4.1 HPCIP - BSIP (Small Solution)

The BSIP is accessible via its factory default IP address 192.168.1.1 in BSIP-Only mode.

To access the BSIP-Only WBM you have to configure an IP address in the network 192.168.1.0/255.255.255.0, e.g. **192.168.1.101** on your maintenance PC.

If the IP address **192.168.1.1** is already **used** in your network, you first have to directly connect the maintenance PC and the BSIP via ethernet. This may be done with a direct ethernet connection via the power injector or via a separate ethernet switch where only the Maintenance PC and the BSIP are connected.

Test via ping, if the BSIP is replying to the ping requests (ping 192.168.1.1).

If not, check all cabling, switch settings, (e.g VLAN configuration).

Ensure that the configured local IP of the maintenance PC adress is up (e.g ping 192.168.1.101).

If you don't get replies consider to reset the BSIP to its factory defaults (see chapter 5.1.9, "Factory reset of BSIP").

Start the Web browser at the Maintenance PC

Access the WBM (Web based management) at the following URL:
http://192.168.1.1
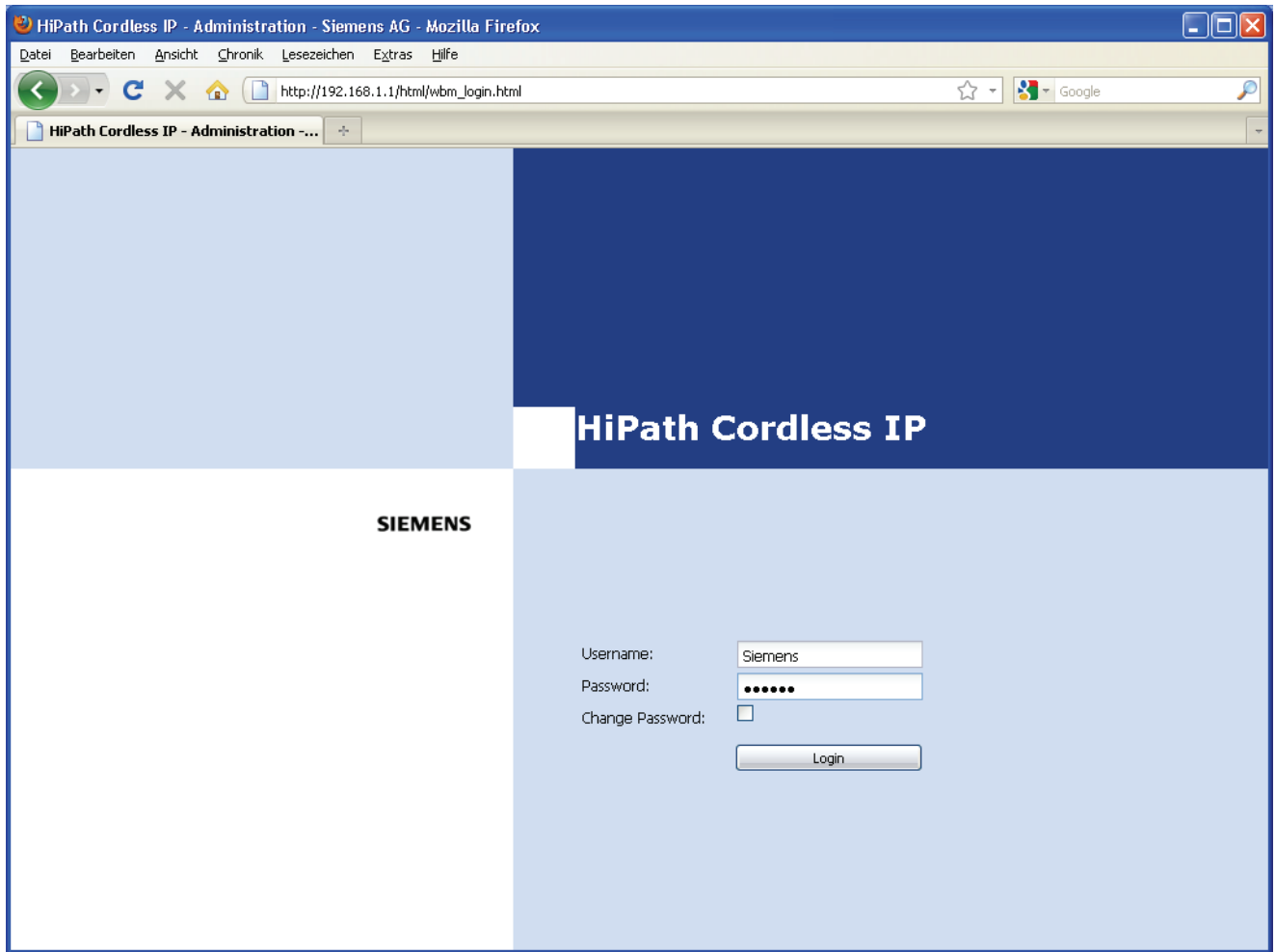
Log in to the WBM with the following (case-sensitive) credentials:

Username: **Siemens**, password: **1q21q2**

Press the [**Login**] button. The configuration page for the BSIP in BSIP-Only mode appears.
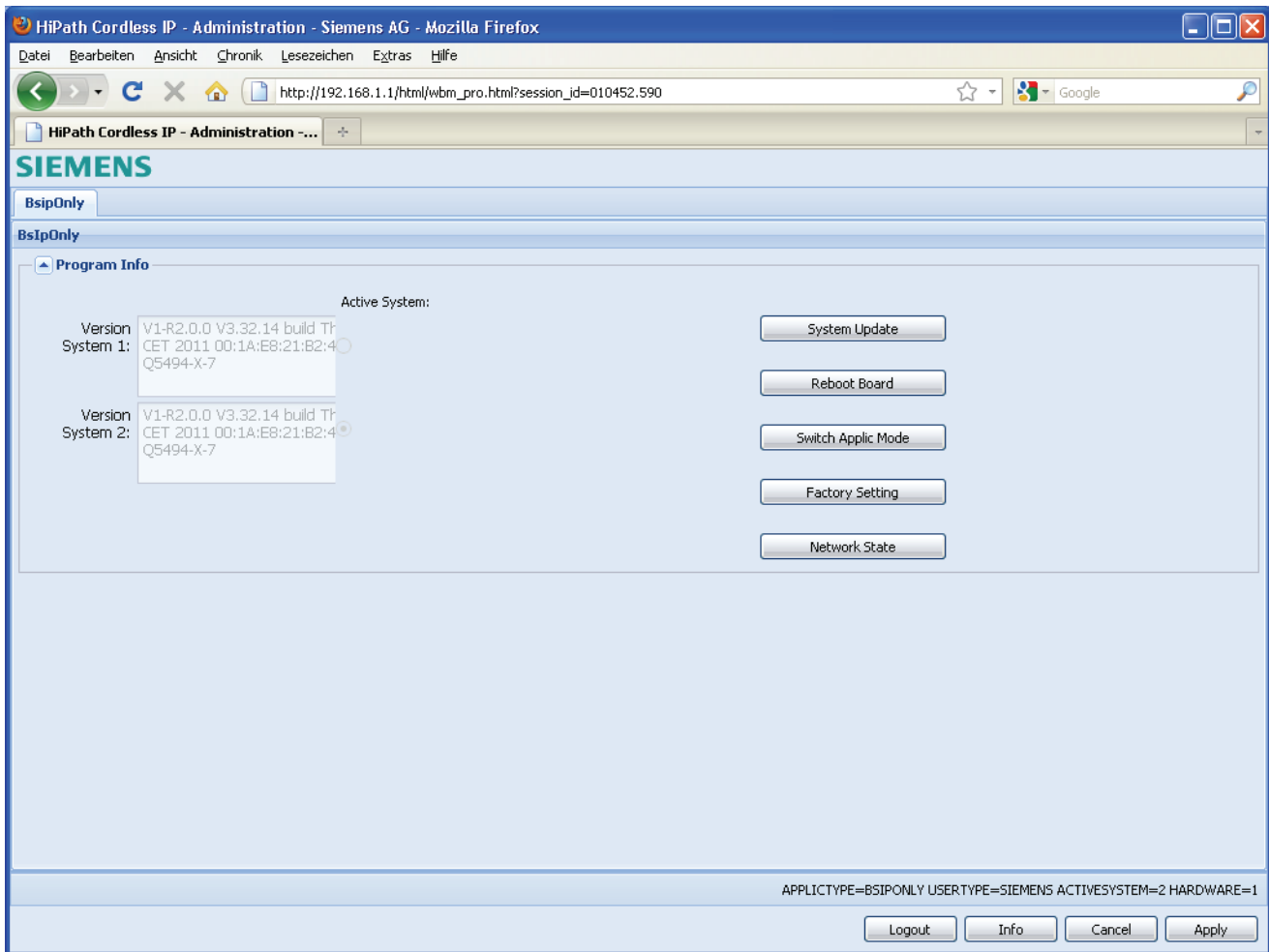
1. To change the application mode of the BSIP from BSIP-Only to BSIP-IWU select [**Switch Applic Mode**].

    • **Hint**: The current application mode is indicated at the bottom status line (APPLICTYPE=BSIPONLY or BSIPIWU)

2. After changing the application mode, the following message box will appear.
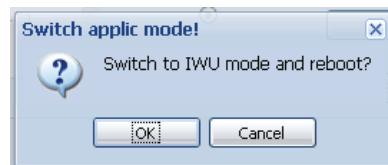
3. Press **[OK]** to reboot the BSIP and start it in application mode BSIP-IWU.

    • **Important note:** After changing the application mode, the BSIP will start in BSIP-IWU mode and therefore has a different default IP address. The default IP address in IWU mode is 192.168.2.1.

The BSIP is accessible via the factory default IP address 192.168.2.1 in BSIP-IWU mode. To access the BSIP-IWU WBM you have to configure an IP address in the network 192.168.2.0/255.255.255.0, e.g. 192.168.2.101 on your Maintenance PC.

1. If the IP address 192.168.2.1 is already used in your network, you first have to directly connect the Maintenance PC and the BSIP via Ethernet. This may be done with a direct Ethernet connection via the power injector or via a separate Ethernet switch where only the Maintenance PC and the BSIP are connected.

2. Test via ping, if the BSIP is replying to the ping requests at ip address (ping 192.168.2.1).
   If not, check all cabling, switch settings, (e.g VLAN configuration).
   Ensure that the configured local IP of the maintenance PC adress is up (e.g ping 192.168.2.101).

3. Start the Web browser at the Maintenance PC

4. Access the WBM (Web based management) at the following URL: http://192.168.2.1

5. Log in to the WBM with the following (case-sensitive) credentials:

   Username: **Siemens**, Password: **1q21q2**

6. Press the [**Login**] button.
   The configuration page for the BSIP in BSIP-Only mode appears.
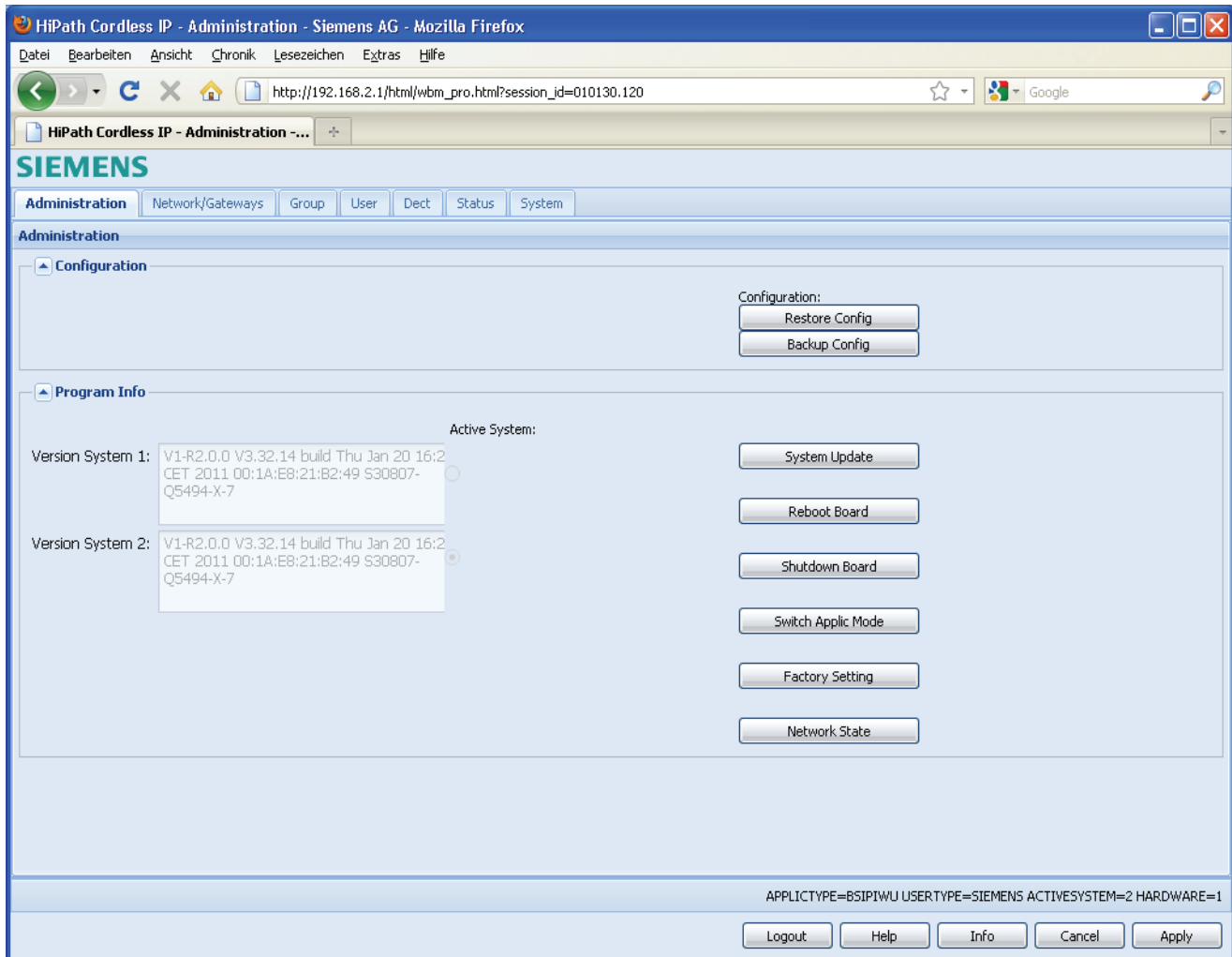
5.2.4.2 HPCIP - Server (Server Solution)

The HPCIP-Server is accessible via its factory default IP address 192.168.2.1. To access the Server WBM you have to configure an IP address in the network 192.168.2.0/255.255.255.0, e.g. 192.168.2.101 on your maintenance PC.

1. If the IP address 192.168.2.1 is already used in your network, you first have to directly connect the maintenance PC and the Server via Ethernet. This may be accomplished by using a direct Ethernet cable or via a separate Ethernet switch where only the Maintenance PC and the Server are connected.

2. Test via ping, if the Server is replying to the ping requests (ping 192.168.2.1). If not, check all cabling, switch settings, (e.g. VLAN configuration). Ensure that the configured local IP of the maintenance PC address is up (e.g.

ping 192.168.2.101).
If you don't get replies you should access the Server locally by keyboard and monitor.

3. Start the Web browser at the Maintenance PC

4. Access the WBM (Web based management) at the following URL:
   http://192.168.2.1

5. Log in to the WBM with the following (case-sensitive) credentials:

   Username: **Siemens**, password: **1q21q2**

6. Press the [**Login**] button.
   The configuration page for the HPCIP Server appears.
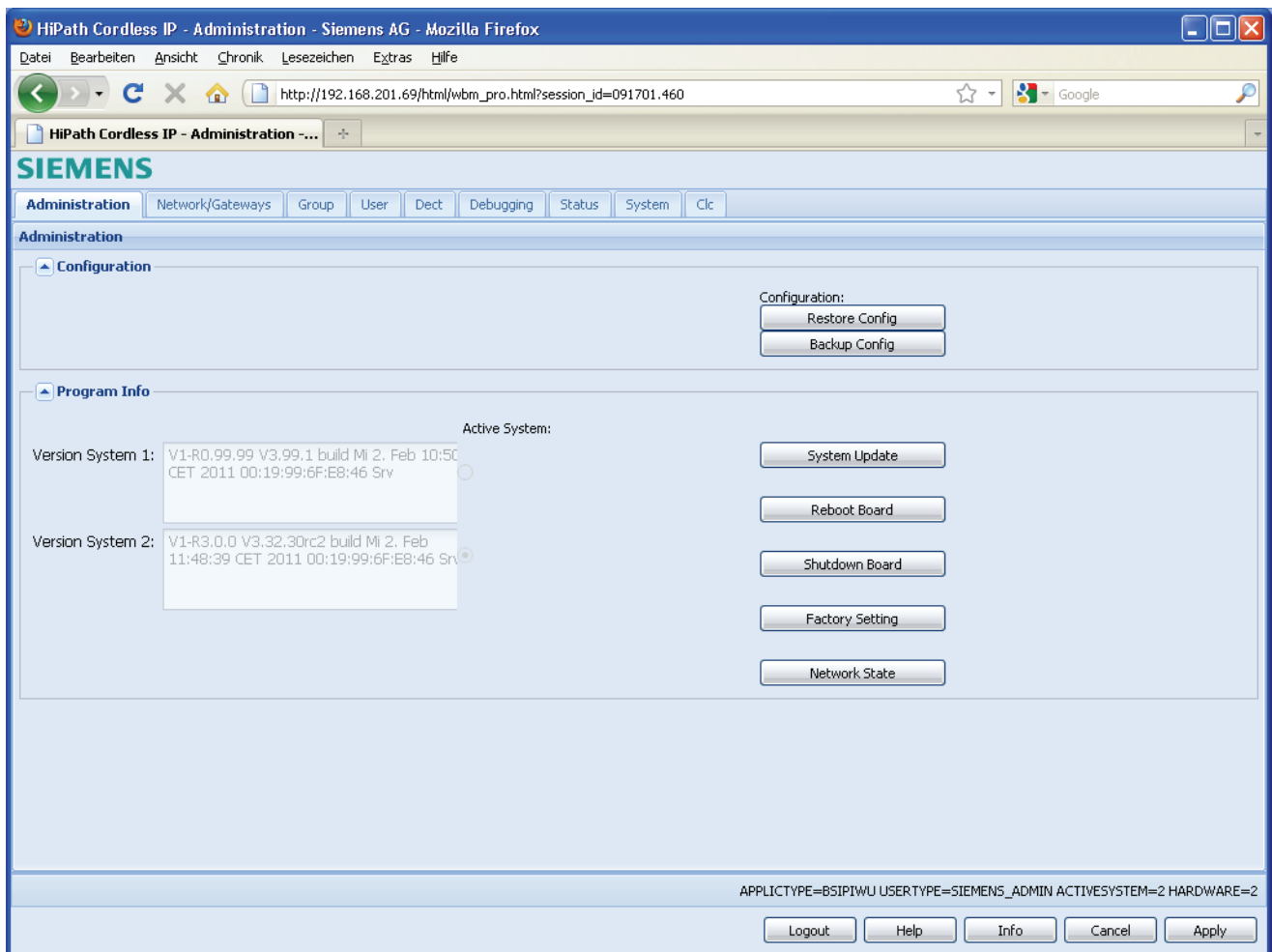
5.2.5 Configuration of VoIP (Infrastructure) network

Since configuration of the IP VoIP (Infrastructure) Network settings requires a reboot of the IWU (BSIP or Server), these settings are configured initially.

To allow direct IP communication between the IWU and the PBX both devices have to be located in the same IP network. Therefore it is necessary to adapt the IP address of the IWU to the network of the VoIP (Infrastructure) . You need at least one unused IP address of the Infrastructure network, which has to be configured at the IWU.

1. Select the configuration page "Network/Gateways".

2. Change the configuration in the bottom frame to the designated values of the IWU.

Ip Address:	192.168.100.1	Network Destination:	0.0.0.0	Tos Value:	Best Effort (0x00) ▼	Time Server IP:	192.168.201.94
Network Mask:	255.255.255.0	Network Mask:	255.255.255.0	Cos Value:	0 ▼	Timezone:	(GMT +01:00) Ams ▼
Default Gateway:	192.168.100.83	Gateway:	0.0.0.0	VLAN Id:	0	Time Server Enable:	☑
		HTTPS Enable:	☑			SNMP Server IP:	0.0.0.0

Change the following values according your needs:

Ip Address:

Here you have to configure the IP address at which the IWU should be available inside the VoIP (Infrastructure) Network. This also is the address at which the BSIP-IWU is accessible via WBM.
This configuration example uses the IP address 192.168.100.1.

Network Mask

Enter the corresponding network mask for the IP address as configured above.

(Default for Class C networks: 255.255.255.0).

This configuration example uses the network mask 255.255.255.0.

Routing Configuration

If routing to another network is necessary (e.g. access from Maintenance PC to IP VoIP (Infrastructure) network) or if infrastructure components (e.g. PBX, NTP or SNMP servers) are located behind other routers, routing may be configured using a "**Default Gateway**" or by a specific network route ("**Network Destination**").

The usage of a "**Default Gateway**" is the recommended routing method.

Using the method "Network Destination", the values for "Network Destination", "Network Mask" and "Gateway" have to be configured. At the Maintenance PC a corresponding route has to be configured.

This configuration example uses the Default Gateway IP address 192.168.100.83.

Time Server Ip

Since the BSIP has no hardware clock, time has to be set according a NTP (or SNTP) time server. After activating the NTP Server at the PBX, it may take some minutes upon activation of the NTP service. This is due to the nature of time synchronisation between NTP server and NTP client.

In contrast to the BSIP, the Server has a built-in hardware clock. However the usage of a accurate time by using NTP is suggested.

This configuration example uses the NTP Server IP address 192.168.201.94.

HTTPS Enable

Activate the https access mode.

Routing entries

If you need routing to another network (e.g. access from maintenance PC to the IP VoIP (Infrastructure) Network, you can configure the corresponding values either by setting the "**Default Gateway**" or by a special "**Network destination**".

If using the "Network destination" method, you have to configure the fields "Network destination", "Network mask" and "Gateway" and additionaly you have to add a route at the maintenance PC.

- **Important**: Ensure that the IP configuration is configured correctly. Otherwise - after rebooting the IWU - it may not be accessible without resetting it to its factory defaults (which have a fixed IP setting of 192.168.1.1 or 192.168.2.1).

5.2.6 Configuration of DECT network

Since configuration of the DECT Network settings requires a reboot of the BSIP, the settings are configured before the BSIP hardware is attached to the designated network segment.

1. Select the the configuration page "Dect".

Server Ip:	192.168.10.1	System Ari:	101b2ff5	VPN Enable:	☐
Network Mask:	255.255.255.0	System Pin:	87654321	VLAN Id:	0
Listen Port:	10500				
IWU as GW:	☑				

2. Change the configuration in the bottom frame to the designated values of the BSIP-IWU.

Server Ip

This field contains the IP address of the server (the IWU) in the DECT network.
It is used for communication between all BSIP-Only and the IWU.

This configuration example uses the Server IP address 192.168.10.1.

Network Mask

In this field the corresponding network mask which is assigned to the Server Ip address is configured. (The default value for a Class-C network is : 255.255.255.0).

This configuration example uses the network mask 255.255.255.0.

System Ari

In this field the System ARI (DECT ID) which has to be unique at each DECT system and has been assigned to the system has to be configured.

This configuration example uses the System ARI 101b2ff5.

System Pin

The "PIN" is a 8-digit number and it is needed for the registration of handsets. It is preconfigured with "00000000" and may be configured systemwide here. You can change the system pin to another decimal value.

This configuration example uses the System Pin "87654321".

IWU as GW

Activate this option to use the BSIP-IWU as a router to the BSIP-Only.

Background: Using the option "IWU as GW" enables the routing (IP forwarding) via the IP VoIP (Infrastructure) Network to the DECT Network. This ensures access to the network in which the BSIP-Only are located, without having an IP address (in the DECT network) configured at the maintenance PC. Additionaly you have to add a route at the maintenance PC

3. Apply the changes by clicking the [Apply] button at the bottom section.
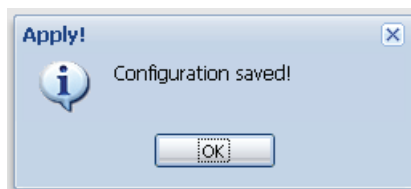
4. Confirm the message box by clicking on **[OK]**.

As stated above, for the changes to become active, the BSIP has to be rebooted.

- **Important:** After rebooting, the IWU will not be accessible by its IP address 192.168.2.1 anymore. Instead it is accessible by the IP address of the IP VoIP (Infrastructure) Network (configured at the step above). If you have attached the IWU directly via a Ethernet cable you have to attach the IWU physically to the designated network segment after rebooting it.

1. Select the configuration page "Administration".

2. Initiate the reboot by clicking the [**Reboot Board**] button.
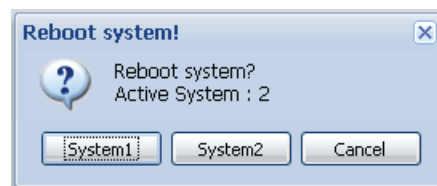
Start the reboot process by clicking on button [System2],if the previously active partition also was System 2 (as this example used - see output of "Active System:"). Otherwise click on button [System1].

Wait about 1 minute for the IWU (BSIP or the Server) to come up again. In case of a BSIP-IWU the board LEDs should change to permanently orange / orange.

3. Access the WBM (Web based management) by the IP address you have configured before for the IP VoIP (Infrastructure) Network.

Depending on the http access mode you have to use http:// or https:// mode

HTTPS Enabled = [   ]use http://{Server Ip of IP VoIP (Infrastructure) Network}

HTTPS Enabled = [X]use https://{Server Ip of IP VoIP (Infrastructure) Network}

Example: https://192.168.201.114

5.2.7 Configuration of users at the PBX

It is assumed that the VoIP users at the PBX are already configured. For detail refer to chapter 5.5, "Configuration Hints for PBXs".

5.2.8 Configuration of users at the BSIP-IWU

5.2.8.1 Gateway and Group

1. Access the WBM of the BSIP-IWU WBM via the web browser at the maintenance PC.

   Example: https://192.168.201.114

2. Log in to the WBM with Username "Siemens".

3. Switch to configuration page "**Network/Gateways**".

4. Add a new gateway entry by clicking on the button [**Add Gateway**].

Enabled	Name	ListenPortR	SIP Server Id	Use OBP	Outbound Proxy	Netmask	DNS SRV	System DNS	DN
☑	OpenScape Office MX 3bx	5060	192.168.201.94	☐	0.0.0.0	255.255.255.0	☐	☐	0.0

Network/Gateways

5. Change the following values:

   Name

   Change the preconfigured name of the PBX to a descriptive name for the VoIP Gateway. This name is only used for the internal configuration of the BSIP Software.

   This configuration example uses the name "OpenScape Office MX 3bx".

   SIP Server Id and Netmask

   Change the preconfigured SIP Server Id from 0.0.0.0 to the IP Address of the used PBX as well as the corresponding "Netmask" to the IP address of your PBX.

   This configuration example uses the IP address 192.168.201.94 and the network mask 255.255.255.0..

6. Switch to configuration page "**Group**"

   Groups are the connecting link between the "Gateways" and the VoIP Users. A User is assigned to a Group and a Group is assigned to a "Gateway".

   The default configuration already contains an entry for a Group, which is used for assigning the Users to the Gateways, so you do not need to make changes here.

7. Add a new group by clicking on the button [Add Group].

8. Change the contents of the following fields.

Name

Change the preconfigured name of the Group (e.g. to the name of the corresponding PBX) . This name is only used for the internal configuration of the BSIP Software.

This configuration example uses the default Group name "default".

Gateways

Select the gateway from the dropdown field which you have configured in the last step.

This configuration example uses the gateway "OpenScape Office MX 3bx".

Intern Call Length

With this setting the maximum number of digits of the calling Party number for internal calls is configured. Calls with a larger number of digits are signaled as external calls at the handset. The default value is "3".

5.2.8.2 User

- **Hint:** Alternatively it is possible to register several users at once using the Bulk Registration Mode. Since this method is out of scope of a quick start, the manual methode is used here.

1. Switch to configuration page "**User**", sub page User ("User -User").

   Set up one or several Users according the user configuration at the PBX for the connection with the BSIP. Please take care of the consistency of the entries between the PBX and the BSIP.

2. Add a new user by clicking on the button [**Add User**].

   - **Hint**: For the correlation of the fields between the BSIP and the PBX refer to chapter 5.5.1.4, "Station Configuration - HPCIP IWU".

3. Change the contents of the following fields:

Msn (necessary)

The MSN has to correlate with the Call number of the User at the PBX.

This configuration example uses MSN 761, 762 and 763.

DisplayName (necessary)

This information is shown at the idle display of the corresponding handset.

This configuration example uses MSN 761, 762 and 763.

Comment (optional)

Here you may enter any desired text for administration purposes.

This configuration example uses the values "Sales", "Marketing" and "Support".

Language

The language used for display messages of the handset can be selected here

This configuration example uses the language "Deutsch".

Groups

Choose a Group (and with that a Gateway) from the dropdown box to which the user is associated to.

This configuration example uses the default Group name "default".

4. Switch to configuration page "User", sub page Voip ("User -Voip").

5. Change the contents of the following fields:

UserName (necessary)

Configure the Name or Number for the registration of the User at the PBX.

This configuration example uses the UserName 761, 762 and 763.

AuthName (optional)

Configure the AuthName which is used for the authentification at the PBX (together with "Password").

This configuration example uses the AuthName 761, 762 and 763.

Password

Optional, but necessary if an "AuthName" is configured; the password which is used for the authentification at the PBX (together with "AuthName").

This configuration example uses the Passwords "1234", "2345" and "3456"..

6. Apply the changes by clicking the [Apply] button at the bottom section.
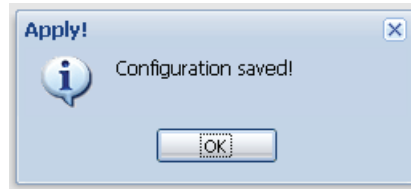
7. Confirm the message box by clicking on **[OK]**.

8. To append further users to the configuration, repeat the steps above.

5.2.9 Configure further BSIP-Only to the system

Attach one further BSIP (for HPCIP-BSIP Solution) or two BSIP (for HPCIP-Server solution) to a PoE port of the network switch of the DECT Network or via a power injector to a standard port of the network switch.

Inside this configuration example the first BSIP (for a HPCIP-BSIP solution the BSIP-IWU) is configured as the synchronization master for the Over-Air synchronization. The second BSIP is configured as synchronization slave..

1. Wait about 2 minutes until the LED states at the BSIP-Only change to permanently green and red.

2. At the WBM of the BSIP-IWU switch to configuration page "**Dect-About**".

3. To scan the newly attached second BSIP click on the button [**Scan**].
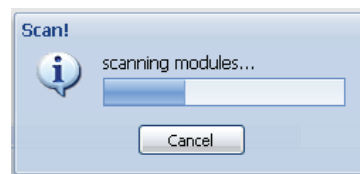
The newly attached BSIP should be found automatically and a record will be appended for it in the table of DECT devices.

Index	Enable	Name	Type	BasestationSe	Version	PartInfo1	PartInfo2	IpAddr Module	IpAddr Server	Server Po	Mac Addr
1	✓	BslpIwuLocal	BslpLocal	000000000	V3.32.14 Jan 20 2011 16:24:11	n/a	n/a	192.168.123.222	192.168.123.111	10500	00-00-00-00-00-00
2	☐	Bslp only	Bslp	738479248	w3.32.14 Jan 20 2011 16:24:51 5	V3.32.14	V3.32.14 Active	192.168.1.1	192.168.2.1	10500	00-1a-e8-21-b0-73

> If the BSIP is not found please read the chapter 5.6, "Troubleshooting / FAQ" concerning possible reasons.

4. At the WBM of the BSIP-IWU switch to configuration page "**Dect-Base**".

5. The BSIP-Only has to be configured for usage within the HiPath Cordless IP system. Select the newly created entry for BSIP-Only and change the contents of the following fields:

Dect-Base

Index	Enable	Name	NumOf	IpAddr Module	Mac Addr
1	✓	BsiplwuLocal	10	192.168.123.222	00-00-00-00-00-00
2	✓	Bslp Room 2.012	10	192.168.10.2	00-1a-e8-21-b0-73

Base | Sync | Ari | About

Enabled (necessary)

Set to Enabled for usage within the HiPath Cordless IP system.

Name (necessary)

Configure a descriptive name for the BSIP. Change the preconfigured name of the BSIP (e.g. to the name of the physical location it is designated for). This name is only used for the internal configuration of the BSIP.

IpAddrModule (necessary)

Configure an IP address for this BSIP inside the DECT network.

- **Hint:** The HPCIP System automatically suggests a valid IP address.

6. At the WBM of the BSIP-IWU switch to configuration page "**Dect-Sync**".

Dect-Sync

Index	Enable	Name	Sync	ParkSync1	ParkSync2	ParkSync3
1	✓	BsiplwuLocal	no	n/a	n/a	n/a
2	✓	Bslp Room 2.012	air	[001] BsiplwuLocal	n/a	n/a

Base | Sync | Ari | About

7. Select the newly created entry for BSIP-Only and change the content of the following fields:

Sync (necessary)

Set to "air" to synchronize the actual BSIP to another BSIP via air.

ParkSync1 (necessary)

Select from the dropdown to which BSIP the selected BSIP should be synchronized to.

This configuration example uses Module "[001] BSIPIWU Local" as the sync master.

8. At the WBM of the BSIP-IWU switch to configuration page "**Dect-Ari**"

9. Select the newly created entry for BSIP-Only and change the content of the following fields:

   Rpn (necessary)

   Change the "Rpn" for the selected first entry from "0" to "1".

   • **Hint:** The HPCIP-System automatically suggests a valid RPN.

   • **Note:** When using several Base Stations they have to be configured with a unique "Rpn" different from "0". Valid RPNs for a class B Ari are 1 ... 255. Using the same RPN as the DECT module number (Index) is very feasible

10. At the WBM of the BSIP-IWU switch to configuration page "**Dect-About**"

The fields "IpAddr Module" and "IpAddr Server" display the current (default) values for the selected BSIP.

To apply all the changes to all BSIP, the BSIP have to be synchronized. During the synchronization process the BSIP-Only will receive its configuration values from the IWU.

11. Apply the changes by clicking the [Apply] button at the bottom section.
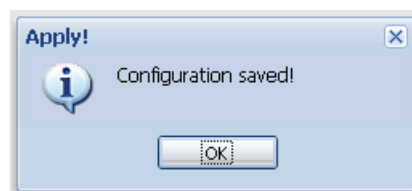
12. Confirm the message box by clicking on **[OK]**.

13. A debug window will appear:
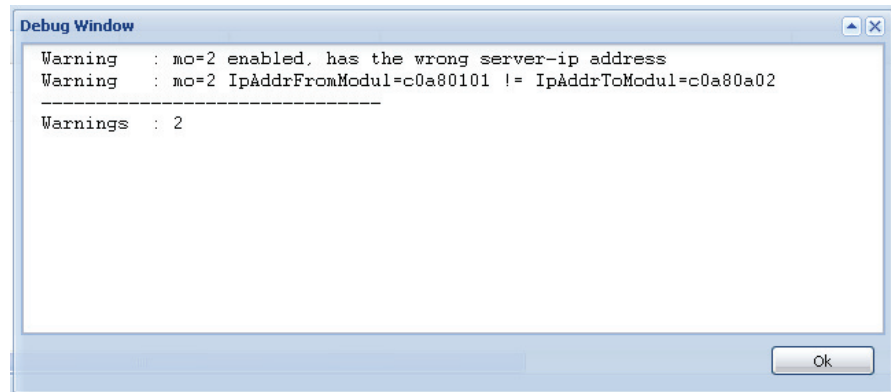
14. Confirm the Debug Window by clicking on **[OK]**.

15. Start the synchronization process by clicking the [**Sync**] button at the bottom section

    A message box will appear:
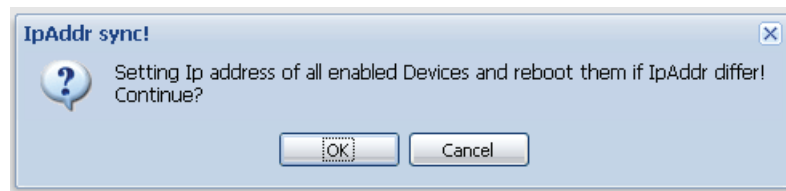
16. Confirm the message box by clicking on **[OK]**.

    The following process will transfer the new settings to all BSIP-Only. Therefore, the BSIP-Only will be rebooted automatically by the system.

    Wait about 2 minutes until the BSIP is started completely (LED states should be green/red).

17. To verify the configured values of the previous steps, click on **[SCAN]**.
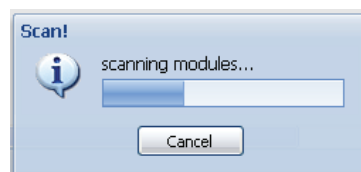
18. At the WBM of the BSIP-IWU switch to configuration page "**Dect-About**".

    Verify, if the values "IpAddr Module" and "IpAddr Server" contain the correct values which have been configured before (IpAddrModule -> IpAddr Module, Server Ip -> IpAddr Server).

5.2.10 Start system services and register handsets

5.2.10.1 Start system services

1. Switch to configuration page "**System**".

   To start the functionality of the BSIP-IWU you first have to start the system services.

2. Start the services by clicking the [**System Start**] button at the bottom section. Starting of the services requires some time.

3. Check if the system services are running by clicking at the [Refresh] button several times.

System				
Enable	Applic Name	Status	Up since	Service
☑	capisrv.exe	Running	23.02.2011 14:54	☐
☑	iwu.exe	Running	23.02.2011 14:54	☐

If the system services are started correctly (both states displayed as "Running", the LED state at the BSIP-IWU should change from orange/orange to green/off.

If a time server is configured correctly and can be contacted, the field "Up since" should display actual local time values, otherwise time will start at "01.01.1970 00:00".

5.2.10.2 Register handsets

- **Hint:** Alternatively it is possible to register several users at once using the Bulk Registration Mode. Since this method is out of scope of a quick start, the manual method is used here.

1. Switch to configuration page "**User-Dect**".

2. Prepare **one handset** for the **registration** process.

   - **Attention:** Do not confirm the following procedure at the Handset right now!
     Start the **Registration procedure** via the **menu at the Handset**. Choose any Base Station for the Registration at the handset. Enter the SystemPIN (preconfigured to "**00000000**" at configuration page "DECT" as PIN at the handset (Attention: Do not confirm yet!).

3. Select the corresponding user in the WBM to which the handset has to be assigned to.

4. Activate the Registration procedure at the WBM by clicking at [**Register**] at the bottom section of page "User-Dect".
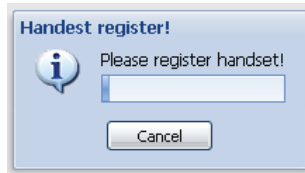
5. Now confirm the already entered PIN at the Handset (normally with softbutton "**OK**").

"The WBM displays the **successful Registration** of the Handset.

- If the handset does not ring please read chapter 5.6, "Troubleshooting / FAQ" concerning possible reasons.

The IPUI of the registered handset is displayed in hexadecimal notation in the user entry.

6. Select the user again and click on [**TestCall**]. The registered Handset will start ringing. You can accept the call at your handset (no voice data will be transferred) or terminate the test call by clicking [**OK**].
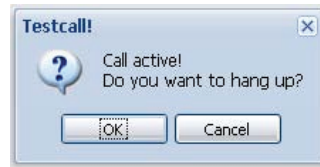
If the handset does not ring please read chapter 5.6, "Troubleshooting / FAQ" concerning possible reasons.

You can register further handsets for already configured VoIP users now or to a later time.

• **Important note**: Telephony functionality is not available before the system services have been started succesfully (Status = Running).

After the services are running, telephony functionality should be available. You should be able to establish calls between the handsets.

5.2.11 "Quick Start" Completion

After you have accomplished some successful test calls you may configure all additional Users and additional BSIP-Only in your System.

At this step it's a good idea to backup the configuration. For details refer to chapter 5.3.3.1.2, "Button [Backup Config]"

5.2.12 Further steps

5.2.12.1 Radio frequency site survey

A radio frequency site survey has to be performed. Within this step, also the synchronisation concept has to be designed, implemented and tested.

5.2.12.2 Synchronisation implementation

The syncronisation implementation should be part of the radio frequency site survey.

For details of synchronisation via air refer to chapter 5.1.4, "Synchronization over air concept".

For details of synchronisation via Ethernet refer to chapter 5.1.5, "Synchronization via Ethernet (acc. IEEE 1588)".

5.3 Configuration reference

For the configuration of the HiPath Cordless IP system you have to connect via a Browser to the BSIP-IWU.

5.3.1 WBM overview IWU

5.3.1.1 Different WBM modes (WBM Users)

- **Hint**: Where not other stated, all documentation is described for WBM mode Siemens Standard.

The system has two built-in factory default WBM users:

WBM mode	Username	Default password
Siemens Standard	Siemens	1q21q2
Siemens Administration	SiemensAdmin	1q21q2

Using the WBM mode Siemens Administration, more or changed configuration options are available.

For most configuration tasks, WBM mode Siemens Standard is sufficient.

5.3.1.2 Features in WBM mode Siemens Admin

Configuration page Network-Gateways

- Fields "Dtmf", "StunnelIp", "LocalIpAddress" available

- Option "Direct Signaling" available

Configuration page User-Dect

- Fields "PnCap" available

- Option "Multi Register" available

Configuration page Dect

- Option "No new modules on scan" available

Configuration page Dect-Radio

- Only available in WBM Mode Siemens Admin

- Field "Diversity" available

- Dropdown Field "Frequency" (Default: "1.88 - 1.90" for Europe, other available values: "1.91 - 1.93"). Changig this option from its default "1.88 - 1.90" is not supported yet.

Configuration page Dect-Ari

- Field "Cipher"

Configuration page Dect-Call

- Only available in WBM Mode Siemens Admin

- Field "NumofChannel" moved from sub-page Base

- Field "Jitter" available

Configuration page Dect-Debug

- only available in WBM mode Siemens Admin

Configuration page Debugging

- only available in WBM mode Siemens Admin

5.3.1.3 Login to WBM

5.3.1.3.1 Multiple WBM sessions

If you login onto the same WBM session on which another user was logged on, you are informed about that by a message box.
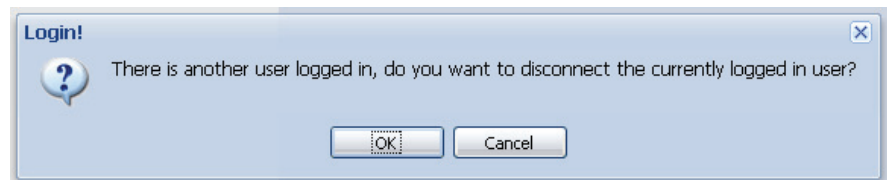
[OK] will logout the currently connected user.

[Cancel] Go back to the Login dialog.

After a timeout of 30 minutes after the last WBM access the user will be logged out automatically by the WBM.

5.3.1.3.2 Login and Password change
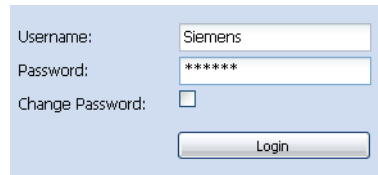
- **Hint**: Password and Username are handled Case sensitive.

The WBM configuration mode is chosen according the Login username.

Concurrent Logins are not possible. The users who tries to login last is given the ability to logout the already logged in user (see above).
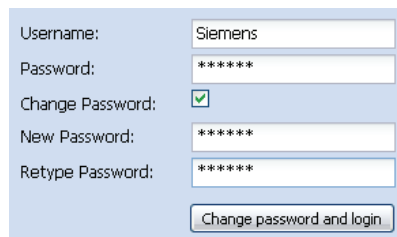
5.3.1.3.3 Changing a WBM User's password

- **Important note:** Please note down the new password at a secure place. Passwords are stored at system level and also used when updating the system at a later time. If you forgot the password, you only may overcome the situation by resetting the system to factory defaults.

1. On the Login page, enter the Username and current password for the destinated user which has to be changed.

Username:	Siemens
Password:	******
Change Password:	☐
	Login

2. Before clicking on [Login] activate the checkbox "Change Password".

3. Two new fields will be displayed: "New password" and "Retype password". Type in the new password in both fields.

   - **Hint**: Username and passwords are case sensitive, the minimum password length is 6 (six) characters.

Username:	Siemens
Password:	******
Change Password:	☑
New Password:	******
Retype Password:	******
	Change password and login

4. Click on [**Change password and login**].

   If both new passwords are equal and valid, you will be logged in onto the WBM. Otherwise a error message will appear.

- **Hint:** A password change is applied to the active system partition. Only after a System update the password changes are transferred to the other system partition.

5.3.1.4 Configuration Objects

The WBM consists of several pages with topically structured configuration options of the IWU Software. These pages can be selected via the Tabs in the upper part of the WBM.

The buttons on all configuration pages on the bottom right have the following meaning:

Logout

This functionality will logout the current user from the WBM session. After you have finished configuration, it is good practice to logout from the WBM session.

Help

The Help button starts the browser based online help system.

Info

Displays current version, license and hardware information as well as the software license agreement.
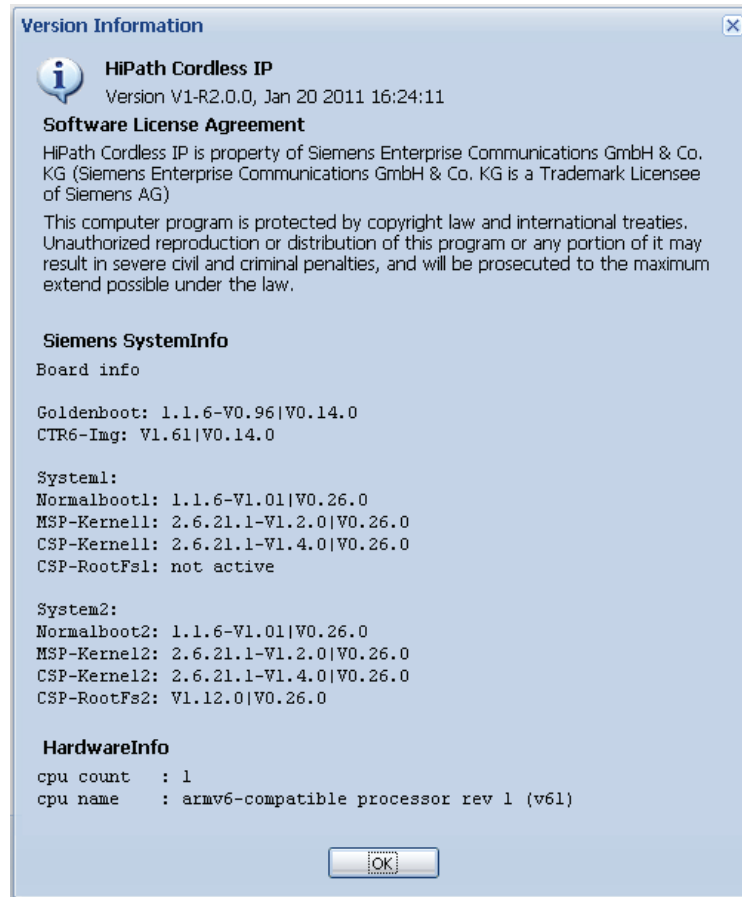
Cancel

By using the **[Cancel]** button, the modifications which have been done since the last [Apply] are discarded.

Apply

With this Button, all WBM configuration is transferred to the Software and will be checked on validity using a validation process (see output of "Debug Window"). If only some WARNINGS are detected, the configuration will be saved. If ERRORS are detected, the configuration is not saved. Observe the ERROR messages in the debug window and apply the necessary changes to the configuration and initiate a new [Apply] process.

5.3.1.5 Configuration Systematic

Several "Gateways" (PBXs) are supported per HiPath Cordless IP system. For establishing a call over a VoIP gateway, a Group has to be assigned to the Gateway and a User has to be assigned to this Group.

The following figure shows the relationships between Gateways, Groups and Users.
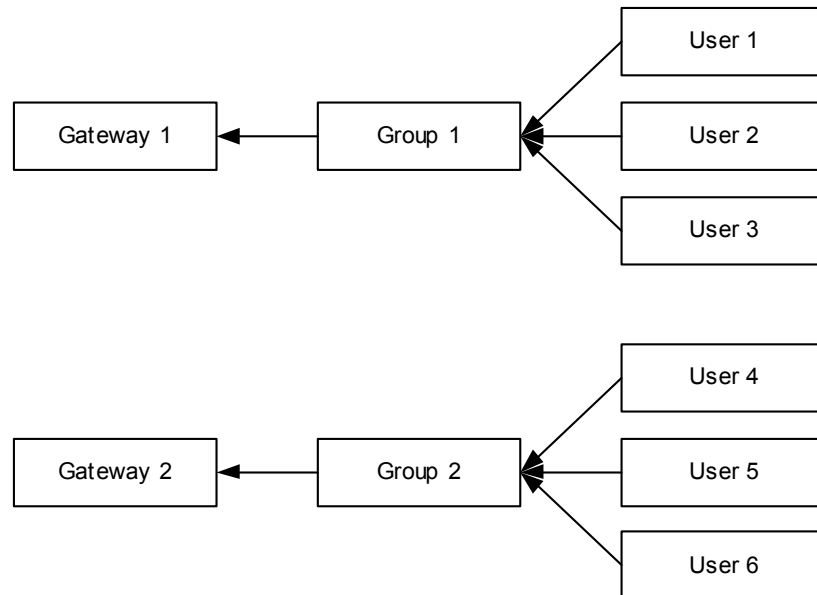
According to the figure above the following relations exist:

- One ore more Users can be assigned to a Group (n:1).

- One Group can be assigned to a Gateway (1:1).

Usually only 1 Gateway (the PBX) is configured for the IP-DECT System.

5.3.1.6 Changing values

Changed values are marked with a red triangle at the top left corner of the corresponding field.

But you have to leave the current field for changes to come in effect (via TAB key or mouse).

Please keep in mind that changes are not in effect immediately.

You have to

1. apply the changes with the **[Apply]** button, for some changes you have to

2. restart the system services or for general configuration changes you have to

3. reboot the IWU

5.3.1.6.1 Debug windows

To inform the user about special events (e.g configuration warnings and/or errors) a Debug window will display the corresponding messages to the user.

After changing (and/or applying) changes to configuration objects, the WBM displays the debug windows with warnings and/or errors.
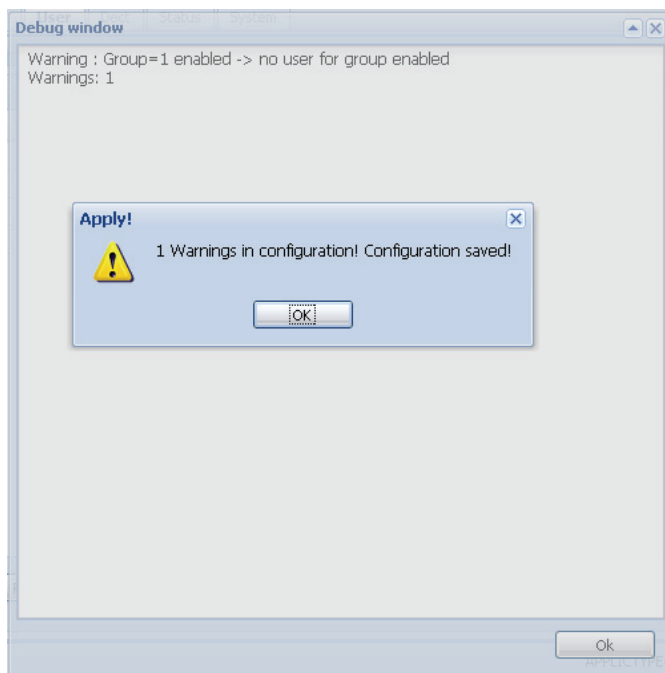
5.3.2 Administration (BSIP-Only)

On the Administration page of the BSIP-Only, administrative configuration and information about the BSIP is provided.
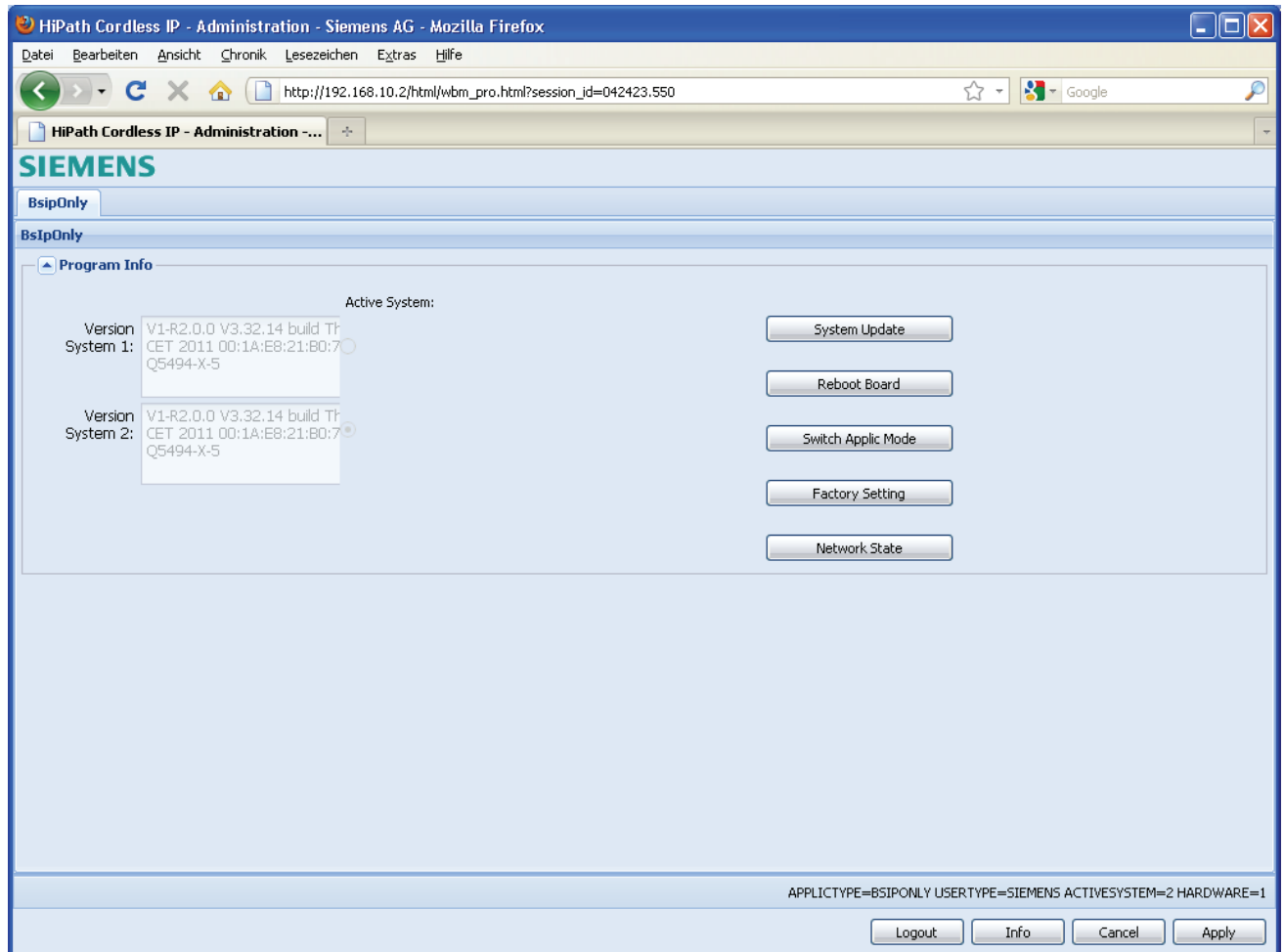
The configuration options are described at chapter 5.3.3, "Administration (IWU)".

The following options differ from the options of a BSIP-IWU:

[**Switch Applic Mode**]

To change the mode of the BSIP between BSIP-Only to BSIP-IWU select [Switch Applic Mode].

Hint: The current working mode is printed out at the bottom status line (APPLICTYPE=BSIPONLY or BSIPIWU) and in the output of [Network State].

After changing the application mode, the following message box will appear.
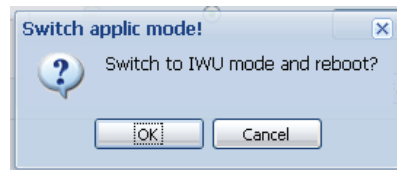
Click on [**OK**] to reboot the BSIP-Only into operation mode BSIP-IWU.

- **Important note:** After switching the Applic mode to BSIP-IWU, the BSIP will obtain the IP configuration which was active the last time it was active in BSIP-IWU mode. This may be the default factory IP configuration for BSIP-IWU mode (192.168.2.1) or another altered IP configuration. The output of the [Network State] displays the IP configuration which will be active after switching to BSIP-IWU mode.

Output of [**Network State**]

```
### Network configurations of BSIP1 ###
## ApplicMode BSIP only ##
## In Iwu mode, the board would start with the following settings ##
## Network / Gateway settings ##
Ip Address            : 192.168.2.1
Network Mask          : 255.255.255.0
Default Gateway       : 0.0.0.0
DHCP enabled          : FALSE
Dns Server 1          : 0.0.0.0
Dns Server 2          : 0.0.0.0

Network Destination   : 0.0.0.0
Network Mask          : 255.255.255.0
Gateway               : 0.0.0.0

Tos Value             : 0
Qos Value             : 0
VLAN Id               : 0

Time Server enabled   : FALSE
Timezone              : GMT+01:00
Time Server Ip        : 0.0.0.0

## DECT settings ##
Server Ip             : 192.168.1.1
Server Network Mask   : 255.255.255.0
Listen Port           : 10500
VPN Enabled           : FALSE
VLAN Id               : 0
IWU as Gw             : FALSE
Dect VPN Enabled      : FALSE

## Dhcp ##
Boottime:
 Status               : unknown
Actual:
 Status               : leasefail
```

5.3.3 Administration (IWU)

On the IWU Administration page, administrative configuration and information about the HPCIP system is provided.
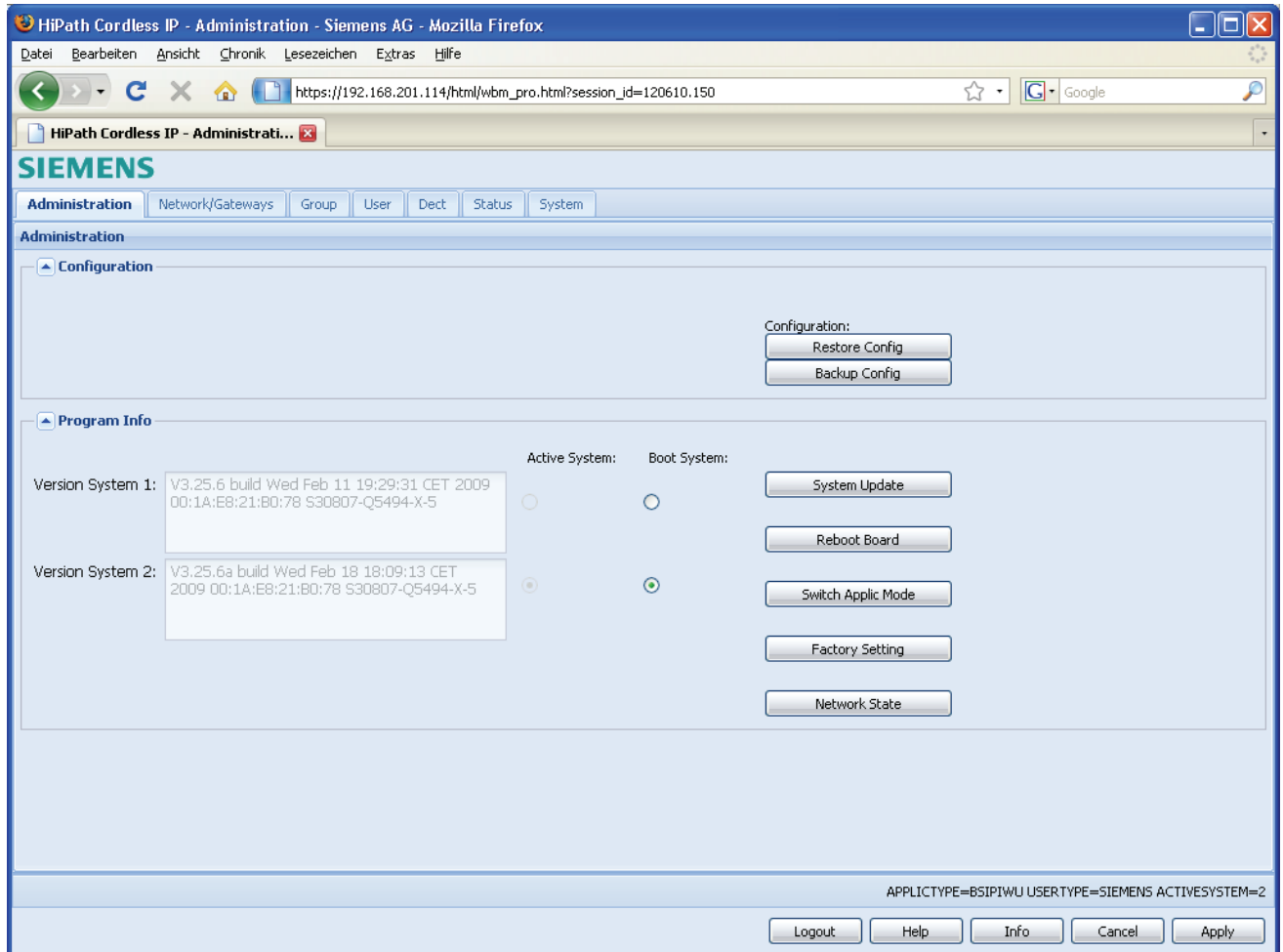
5.3.3.1 Frame Configuration

5.3.3.1.1 Button [Restore Config]

1. With the Button [**Restore Config**] the complete configuration of the BSIP-IWU can be restored from a previously backuped configuration from a file.

• **Hint**:The system services have to be stopped to use this feature.
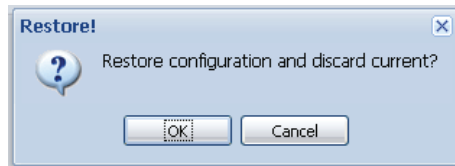
2. After confirming the action with button **[OK]**, a file "Restore Configuration" Dialog opens.
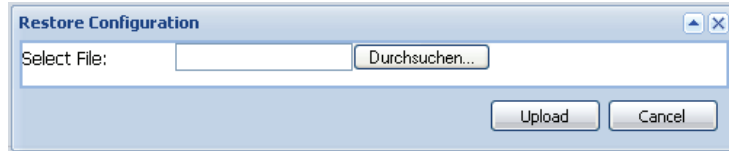
3. After clicking on [**Durchsuchen**] you can select a configuration file using a browser based file open dialog. (by default "iwu_config.tgz").

4. After you have selected the desired configuration file you can load it into the IWU using the [**Upload**] button.
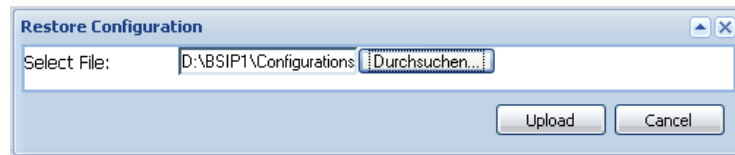
During the upload process, a message box with a progress bar will be displayed.
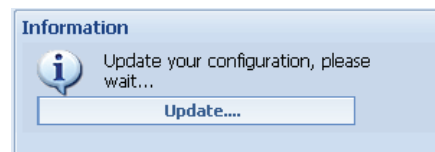
•   **Important:** All stored configuration is loaded into the WBM. Ensure that you have loaded the correct configuration file. Particularly ensure that all relevant IP address values are correct (otherwise you won't be able to access the WBM after a reboot).

5. After the configuration file is downloaded, you have to apply or discard the changes. For both actions, a reboot has to be performed.

5.3.3.1.2 Button [Backup Config]

With this Button the complete configuration of the IWU can be backuped and stored on the file system of the maintenance PC.

1. After clicking on the button [**Backup Config**], a browser based file open dialog will be displayed immediately.
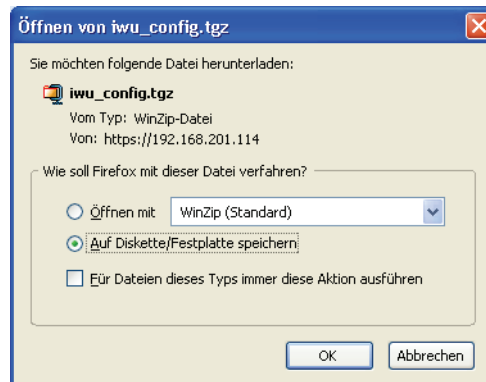
2. You have to select the store method of the dialog, click on button **[OK]** and select from the following "save as" dialog a folder to store the configuration files on the maintenance PC or a directory available via the network.
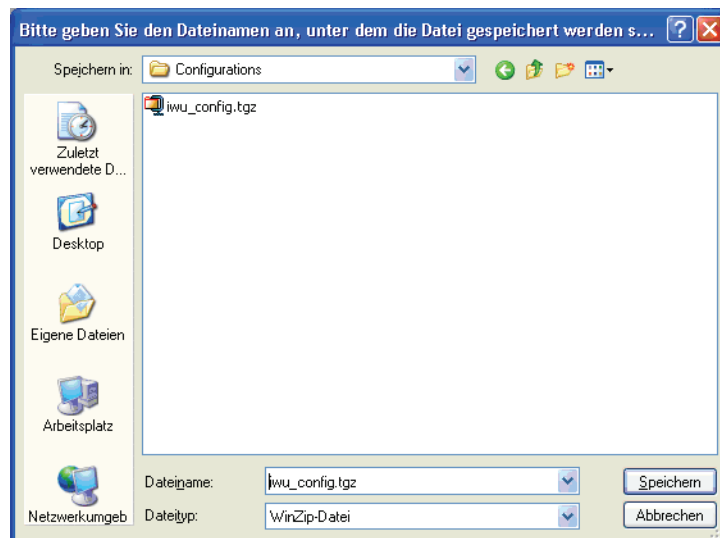
3. Save the configuration file using the default name "iwu_config.tgz " or change it according to your needs (Don't use blanks in the filename).

5.3.3.2 Frame Program Info

Version System 1 and Version System 2

System1 and System2 partitions

To guarantee a functional BSIP or IWU at any time, two bootable systems are present on the BSIP:

• The current (active) system and

• the fallback (non active) system.

Therefore the BSIP and the Server-IWU have two different systems partitions:

• System 1 and

• System 2.

Version System x:

Displays information about software (version number and date) and hardware (MAC address, part number, revision of hardware, e.g. "X-7").

Active system

The radio buttons below "Active System" indicate, which of the both System partition is the currently ACTIVE System partition. In the example of the screenshot above, System 2 is the active partition.

• **Hint**: Don't activate a system partition which displayed version is "n/a" or "update unsuccessfull". This may lead to an unusable system.

5.3.3.2.1 [System Update]

Updating the HPCIP system software

Important notes:

- If you update the system software, the Update is always applied to the NON-active system partition.

- Furthermore, the current configuration of the active system will be applied to the NON-active system partition.

- You have to ensure to use the SAME software version at all BSIPs. Therefore, updating the software has to take place at the BSIP-IWU AND at all BSIP-Only.

- A downgrade is not fully supported. In need of a downgrade, a factory reset is applied automatically. Please refer to the delivered Release notes of the new version for details of the update process.

- Create a backup of the old configuration (Page Registration - [Backup Config]).

- An update may be performed only, if the partitions of all enabled BSIP are synchronous to the current partition of the IWU. Otherwise the BSIP have to be updated manually or have to be synced using the [SYNC] button and afterwards have to be booted into the same system partition by rebooting the IWU.

Update instructions

1. Please create a backup of the old configuration (Page Registration - [Backup Config].

2. Ensure that you have a firmware file of the old version available (in case of a necessary downgrade).

3. Start with the update for the IWU. All enabled BSIP are updated automatically.

4. After finishing the update process, reboot the IWU.

5.3.3.2.2 Other options

[Reboot Board]

After clicking the button [Reboot Board] a dialog appears where you have to select the partition which should be active after the reboot.
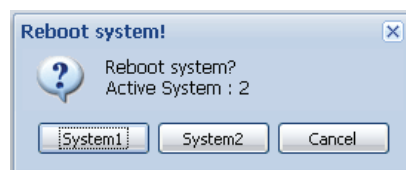
The current partition number is displayed separately (see "Active System: 2" in this example).

By clicking on [System1] the IWU will reboot and started with "System 1" as the active partition.

By clicking on [System2] the IWU will reboot and started with "System 2" as the active partition.

By clicking on [Cancel] the dialog will be closed.

[Shutdown Board] (only for Server-IWU)

By using this functionality the Server-IWU may be shut down and the server will be switched off automatically.

[Switch Applic Mode] (only for BSIP)

To change the mode of the BSIP between BSIP-Only to BSIP-IWU select [Switch Applic Mode]. Afterwards the BSIP will be rebooted.

*   **Hint**: The current working mode is printed out at the bottom staus line (APPLICTYPE=BSIPONLY or BSIPIWU) and in the output of [Network State].
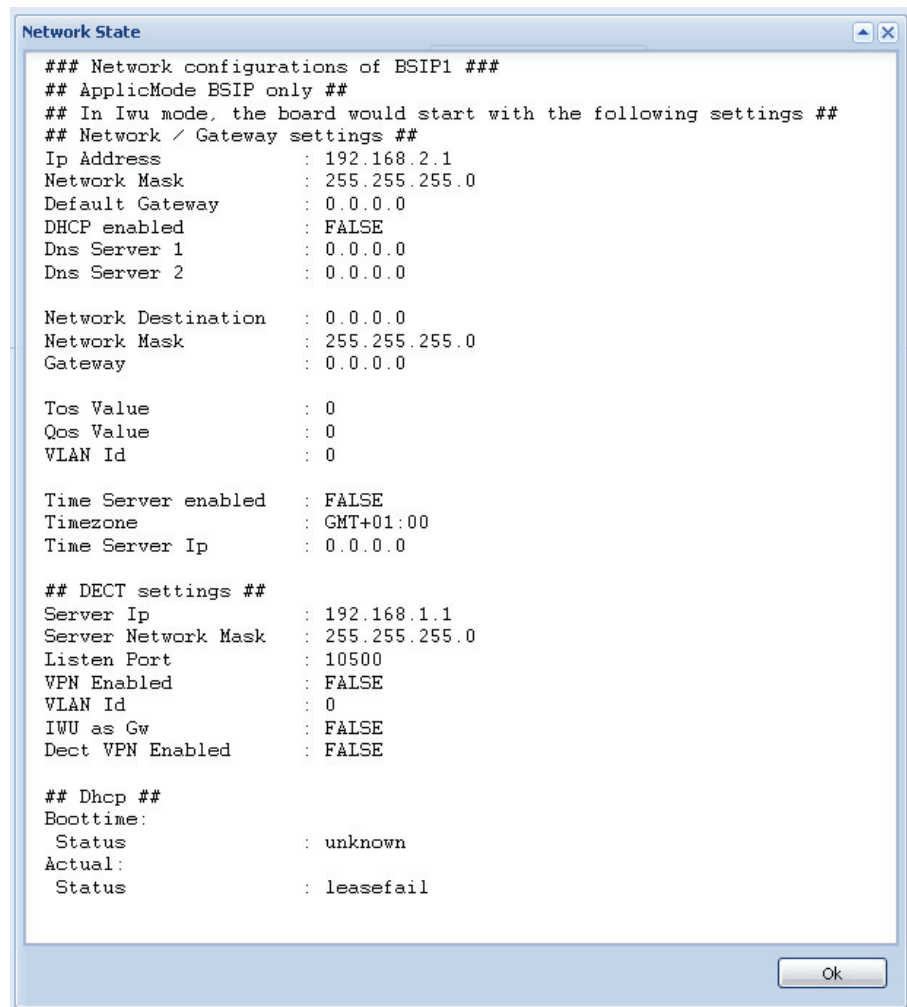
After changing the application mode, the following message box will appear.

Press **[OK]** to reboot the BSIP and start it in the other application mode.

*   **Important note**: After changing the application mode the BSIP will start with the IP configuration which was configured last for the corresponding application mode. This may be the default configuration for the mode or the already configured addresses for the mode.

[Factory setting]

Using this functionality, a factory reset may be initiated.

For a BSIP this functionality may be used alternatively to the procedure of factory reset by power sequencing described in chapter 5.1.9, "Factory reset of BSIP".

[Network State]

By clicking on button [Network states] a new windows will be opened which displays summarized information about the network settings.

Simultaneously a DHCP request will be initiated. Further details may be found in chapter 5.3.4.2, "Network configuration" and chapter 5.4.1.2, "DHCP".

The Network State also displays the status of the SIP Survivability parameters. For details refer to Chapter 5, "SIP Survivability".

```
Network State                                    Active System:                        ▲

    ### Network configurations of BSIP1 ###
    ## ApplicMode Iwu ##
    ## Network / Gateway settings ##
    Ip Address          : 192.168.100.1
    Network Mask        : 255.255.255.0
    Default Gateway     : 192.168.100.83
    DHCP enabled        : FALSE
    Dns Server 1        : 192.168.100.251
    Dns Server 2        : 192.168.100.252

    Network Destination : 0.0.0.0
    Network Mask        : 255.255.255.0
    Gateway             : 0.0.0.0

    Tos Value           : 0
    Qos Value           : 0
    VLAN Id             : 0

    Time Server enabled : TRUE
    Timezone            : GMT+01:00
    Time Server Ip      : 192.168.201.94

    ## DECT settings ##
    Server Ip           : 192.168.10.1
    Server Network Mask : 255.255.255.0
    Listen Port         : 10500
    VPN Enabled         : FALSE
    VLAN Id             : 0
    IWU as Gw           : TRUE
    Dect VPN Enabled    : FALSE

    ## Dhcp ##
    Boottime:
     Status             : disabled
    Actual:
     Status             : valid
     Ip Address         : 192.168.100.220
     Network Mask       : 255.255.255.0
     Default Gateway    : 192.168.100.101
     Dhcp Server        : 192.168.100.101
     Dns Server 1       : 192.168.100.101
     Dns Server 2       : 0.0.0.0

    ## Gateway ##
    001: <        OpenScape Office MX 3bx> Ip 1 : <192.168.201.94>:5060
    002: <        OpenScape Office MX 1bx> Ip 1 : <192.168.201.93>:5060



                                                          [ Ok ]
```

5.3.4 "Network/Gateways" Configuration (IWU)

The configuration page "Network/Gateways" is divided into two parts.

Enabled	Name	ListenPortRemote	SIP Server Id	Use OBP	Outbound Proxy	Netmask	DNS SRV	System DNS	DNS 1	DNS 2	Dtmf	Stunnellp	LocallpAddress
☑	OpenScape Office MX 3bx	5060	192.168.201.94	☐	0.0.0.0	255.255.255.0	☐	☐	0.0.0.0	0.0.0.0	RTP	0.0.0.0	0.0.0.0
☑	OpenScape Office MX 1bx	5060	192.168.201.93	☐	0.0.0.0	255.255.255.0	☐	☐	0.0.0.0	0.0.0.0	RTP	0.0.0.0	0.0.0.0

[Add Gateway] [Delete Gateway]

Ip Address:	192.168.100.1	Network Destination:	0.0.0.0	Tos Value:	Best Effort (0x00)
Network Mask:	255.255.255.0	Network Mask:	255.255.255.0	Cos Value:	0
Default Gateway:	192.168.100.83	Gateway:	0.0.0.0	VLAN Id:	0
DHCP Enable:	☐	HTTPS Enable:	☑	Direct Signaling:	☐
System DNS 1:	192.168.100.251				
System DNS 2:	192.168.100.252				

Time Server IP:	192.168.201.94
Timezone:	(GMT +01:00) Ams
Time Server Enable:	☑
SNMP Server IP:	0.0.0.0

APPLICTYPE=BSIPIWU USERTYPE=SIEMENS_ADMIN ACTIVESYSTEM=2 HARDWARE=1

[Logout] [Help] [Info] [Cancel] [Apply]

In the table view at the top, the VoIP gateways (PBX) are assigned to the "VoIP" connections.

At the bottom of the page, the general network configuration of the BSIP-IWU network is done.

5.3.4.1 Gateway configuration

- **Hint**: To add or delete a Gateway entry, the system services have to be stopped before. All changes will be activated after a restart of the system services.

1. To add a new entry for a gateway, click on [**Add Gateway**]. A new entry line
    with default values is appended, which have to be modified according to your
    system needs.

    The new entry line is either inserted above the selected Gateway or inserted
    at the top of the list if no Gateway is selected.

2. A selected Gateway entry may be deleted by clicking [**Delete Gateway**].

The columns of the configuration page have the following meaning:

Enabled

When activating this element the selected Gateway (the PBX) is added to the
configuration and can be selected when configuring the Groups later on.

Name

Enter a unique name here for the Gateway. This name will be displayed in the
dropdown box of the available Gateways when configuring the Groups.

ListenPortRemote

This entry determines the common SIP listen port of the configured gateway.
There is no need to change this port to another value than 5060. The default
setting is "5060".

SIP Server Id

The value is equal to the IP address of the VoIP Gateway (SIP Server for INVITE
and REGISTER Messages). It shall be located in the IP Infrastructure network
(see chapter 5.1.3, "Network Concept").

If a domain name is configured, the HPCIP system will try to resolve this name
into an IP address by means of a DNS query if option "Use OBP" is deactivated.
If option "Use OBP" is activated, the name is not resolved by DNS.

If a DNS request delivers several IP addresses, the first IP address in this list will be used and all others IP addresses will be ignored. The DNS request will be repeated hourly. If the IP address is changed by a DNS request, this IP address will be used as soon as a user looses his RAS registration or a call establishment will timeout.

Use OBP

This option is used to control the usage of a SIP Outbound Proxy (e.g. Openscape Branch).

If this checkbox is **activated**, a valid IP address has to be entered in the column "Outbound Proxy". This IP address will be used for the Layer 3 Signaling (IP header).

If the Checkbox is **deactivated**, the column "Outbound Proxy" will be ignored. In this case the value of column "SIP Server Id" will be used for Layer 3 Signaling.

Outbound Proxy

Configures the IP address of the SIP Outbound Proxy. This IP address will be used for the Layer 3 Signaling (IP header).

It shall be located in the IP Infrastructure network (see chapter 5.1.3, "Network Concept"). At the IWU a corresponding IP Infrastructure address has to be configured.

Netmask

Enter the netmask for the IP address for the Gateway here. (Default for Class C networks: 255.255.255.0).

DNS SRV

Controls the usage of DNS Service Records. For detail refer to chapter 5.4.1.7.3, "DNS SRV".

If the checkbox "DNS SRV" is **activated**, the columns "Outbound Proxy" and "ListenPort Remote" will be ignored for this gateway. The SIP Server addresses are now derived by DNS SRV requests. Therefore the column "SIP Server Id" must contain a valid domain name. The DNS request will be repeated hourly.

If the checkbox "DNS SRV" is **deactivated**, the columns "Outbound Proxy" and "ListenPort Remote" will be used for this gateway.

The maximum number of SIP Server addresses per gateway will be limited to 5.

System DNS

This option determines, if the global DNS servers ("System DNS 1" and " System DNS 2") or gateway specific DNS servers ("DNS 1" and "DNS 2") are used.

If the checkbox "System DNS" is **activated**, the gateway specific DNS Server "DNS 1" and "DNS 2" are ignored. Instead, the System Global DNS Server ("System DNS 1" and " System DNS 2") are used.

If the checkbox "System DNS" is **deactivated**, the gateway specific DNS Server "DNS 1" and "DNS 2" may be configured, which are used for DNS queries for this specific gateway.

DNS 1

If the option "System DNS" is deactivated, the IP address of the primary DNS server for the current PBX may be configured here.

DNS 2

If the option "System DNS" is deactivated, the IP address of the secondary DNS server for the current PBX may be configured here.

Dtmf (only available in advanced Config. Mode)

Selects the method for the transmission of DTMF digits ("tones") to the Gateway:

"Signaling": The DTMF Digits are transmitted via the Signaling protocol to the Gateway (For SIP via the INFO method).

"RTP": The DTMF Digits are transmitted to the Gateway via the Voice (RTP) channel (e.g. for SIP embedded in the RTP protocol according to RFC2833).

There is no need to change this setting for the supported gateways. The default setting is "RTP".

Stunnel IP (only available in advanced Config. Mode)

Optional - The ip address of the Stun Server for the VoIP gateway SIP Registrar or the Proxy Server. This configuration is depending on the used PBX. There is no need to change this setting for the supported gateways. The default setting is "0.0.0.0".

LocalIPAddress (only available in advanced Config. Mode)

Optional IP address to which the communication to the gateway should be bound to. There is no need to change this setting for the supported gateways. The default setting is "0.0.0.0".

5.3.4.2 Network configuration

At the bottom of the configuration page "Network/Gateways", the general network configuration of the BSIP-IWU network is done.

Refer to the concepts of networking described in chapter 5.1.3, "Network Concept".

- **Hint**: All changes will be activated after a reboot of the BSIP.

Ip Address:	192.168.100.1	Network Destination:	0.0.0.0	Tos Value:	Best Effort (0x00)	Time Server IP:	192.168.201.94
Network Mask:	255.255.255.0	Network Mask:	255.255.255.0	Cos Value:	0	Timezone:	(GMT +01:00) Ams
Default Gateway:	192.168.100.83	Gateway:	0.0.0.0	VLAN Id:	0	Time Server Enable:	☑
DHCP Enable:	☐	HTTPS Enable:	☑	Direct Signaling:	☐	SNMP Server IP:	0.0.0.0
System DNS 1:	192.168.100.251						
System DNS 2:	192.168.100.252						

IP settings for IWU

Ip Address

Here you have to configure the IP address at which the BSIP-IWU should be configured inside the VoIP (Infrastructure) Network. This is also the IP address at which the BSIP-IWU is accessible via WBM.

The factory default IP address is 192.168.2.1. This IP address may not be used for furthrt configuration of the IWU.

Hint: The configured IP address may NOT be located inside the DECT network. For details refer to chapter "4.2.1 Free IP Addressing".

Network Mask

Enter the corresponding netmask for the IP address as configured above. (Default for Class C networks: 255.255.255.0).

Default Gateway

If all other routing is done via a default gateway , it can be configured here. Alternatively, a dedicated route may be configured using the settings "Network destination", "Network Mask" and "Gateway" as described below.

- **Important:** All BSIP devices must be located inside the same network segment and therefore **MUST NOT** be separated by layer 3 Routing devices. Only Layer 2 switches are supported between the BSIP.

DHCP Enable

Activate this option if the BSIP VoIP (Infrastructure) network has to be configured by a DHCP server. For DHCP details refer to chapter "x.x.x DHCP".

- **Important notes:**

  - If using DHCP for the VoIP (Infrastructure) network, the configuration of the DECT network has to be done manually (since configuration of DECT IP addresses may not be distributed by the DHCP server).

  - After applying the DHCP changes (reboot of IWU), the IWU will be assigned a new IP address by the DHCP server. Since there is no local console access at BSIP possible, the only method to get the assigned IP address is to have access to the DHCP servers lease information! Contact the administrator of the DHCP server before activating this option.

  - The last assigned IP addresses may be derived by the output of [Network State] which simultaneously initiates a new DHCP request.

  - Alternatively, a dedicated route to another network segment which is not reachable by the default gateway may be configured using the settings "Network destination", "Network Mask" and "Gateway" as described below.

Network Destination

Using this field, the destination address for the other IP network (e.g. 192.52.109.0) may be configured.

Network Mask

Using this field, the corresponding network mask for the "Network destination" (e.g. 255.255.255.0) may be configured.

Gateway

Using this field the IP address of the gateway inside the VoIP (Infrastructure) network which handles the routing to the other network may be configured.

HTTPS Enable

Determines if https (Hypertext Transfer Protocol over Secure Socket Layer) should be used for WBM communication between the browser and the BSIP. Using https encrypts the communication between the browser and the WBM. It is suggested to use https mode.

Depending on the http access mode you have to use http:// or https:// mode at the browser.

HTTPS Enabled = [ ]   use **http://**{Server Ip IP VoIP (Infrastructure) Network}

HTTPS Enabled = [X]   use **https://**{Server Ip IP VoIP (Infrastructure) Network}

Example: **https://192.168.201.114**

Tos Value

With the "TOS Value" you can configure the prioritization of the IP packets via TCP/IP (Layer3) according to DSCP. It is only used for the IP DSCP field for VoIP Signalling (SIP) and VoIP data (RTP) packets towards the PBX (VoIP Infrastructure Network).

Other IP packets e.g.

• WBM or SSH towards the VoIP Infrastructure network or

• packets between BSIP-Only and BSIP-IWU (DECT Network)

are **NOT** tagged with configured the DSCP value. (Default = "0", i.e. no prioritization).

Using the dropdown you may select one of the pre-configured ToS values.

Cos Value

With the "CoS Value" (Class of Service) you can configure the prioritization of the Ethernet packets via Ethernet (Layer2) according to 802.1p. (Default = "0", i.e. no prioritization).

Using the dropdown you may select one of the pre-configured CoS values.

VLAN Id

The corresponding VLAN Id (according IEEE 802.1q) for the VoIP (Infrastructure) network is configured here.

VLAN configuration is activated, if the VLAN Id is configured to a valid VLAN Id unequal to 0.

If VLAN is activated, the IWU sends and expects tagged Ethernet packets. Therefore the switch port to which the IWU (BSIP-IWU or SERVER-IWU) is connected to, has to be configured to tag the Ethernet frames with the VLAN Ids. Tagging has to be established for the VLAN Id of the VoIP (Infrastructure) network (this VLAN Id) AND for the VLAN Id of the DECT network.

• **Important note:** In contrast to a IWU (BSIP-IWU or Server-IWU), the BSIP-Only is not able to handle tagged Ethernet packets. For this reason, the Switchport - at which a BSIP-Only is attached to - has to be configured untagged.. For details refer to option "Vlan Id" of the DECT network at chapter 5.3.7.8.2, "General configuration options".

All Ethernet frames towards the VoIP (Infrastructure) network between the IWU and the Ethernet switch are tagged with the configured VLAN Id configured for the Infrastructure network (option "VLAN Id" at page Network/Gateways - this option).

All Ethernet frames towards the DECT network between the IWU and the Ethernet switch are tagged with the configured VLAN Id configured for the DECT network (option "VLAN Id" at page DECT).

Please take account of the correlating VLAN configuration of the DECT network at chapter 5.3.7.8.2, "General configuration options".

Direct Signaling

This option determines, if incoming INVITES from unknown (unconfigured) PBX IP address are accepted or rejected.

If this flag is disabled, HPCIP accepts only calls from the IP-address where the user is registered to. This is the default setting.

If this flag is enabled HPCIP accepts calls from any IP addresses.

Usage of this option is needed if the IWU is directly connected to geographically node separated OSV cluster (Main-Office, no OpenBranch-Proxy involved). For security reasons this flag should only be enabled in a Geo-separated OSV setup.

Time Server IP

The IP address of the Time Server is configured here.

Since the BSIP has no hardware clock, the time has to be set by contacting a NTP (or SNTP) time server. In contrast to the BSIP, the Server has a built-in hardware clock. However the usage of an accurate time by using NTP is suggested

- **Hint:** Some supported PBX platforms may serve as a (S)NTP server. For details refer to e.g chapter 5.5.1.5, "Time server configuration".

If a time server is not configured correctly and cannot be contacted, local time will start at "01.01.1970 00:00".

Timezone

If using a Time Server, the timezone has to be configured according the physical location of the HiPath Cordless IP solution (country). Since NTP is always using UTC time, the local time has to be calculated against the time zone information to get correct current Local time.

Time Server Enable

Enables the usage of the Time Server.

After activating the NTP Server at the PBX it may take some minutes upon activation of the NTP service. This is due to the nature of time synchronisation between NTP server and NTP client.

SNMP Server IP

Using this option, an IP address of a SNMP server may be configured here to which SNMP traps are being send. For details refer to chapter 5.4.1.1, "SNMP".

System DNS 1

In this field the IP address of the first (primary) system global DNS server is configured.

If this server is unreachable, the system uses "System DNS 2". This address may also be based on DHCP if it is a component part of "DHCP-Offer".

For details refer to chapter 5.4.1.7.2, "DNS Administration".

System DNS 2

In this field the IP address of the second (secondary) system global DNS server is configured.

This server is used by the system, if the first (primary) DNS Server is unreachable. This address may also be based on DHCP if it is a component part of "DHCP-Offer".

For details refer to chapter 5.4.1.7.2, "DNS Administration".

5.3.5 "Group" Configuration (IWU)

On the configuration page "Group" the Groups are defined, which are the connecting link between the "VoIP Users" and the "Gateways". A User has to be assigned to a Group and a Group has to be assigned to a Gateway.
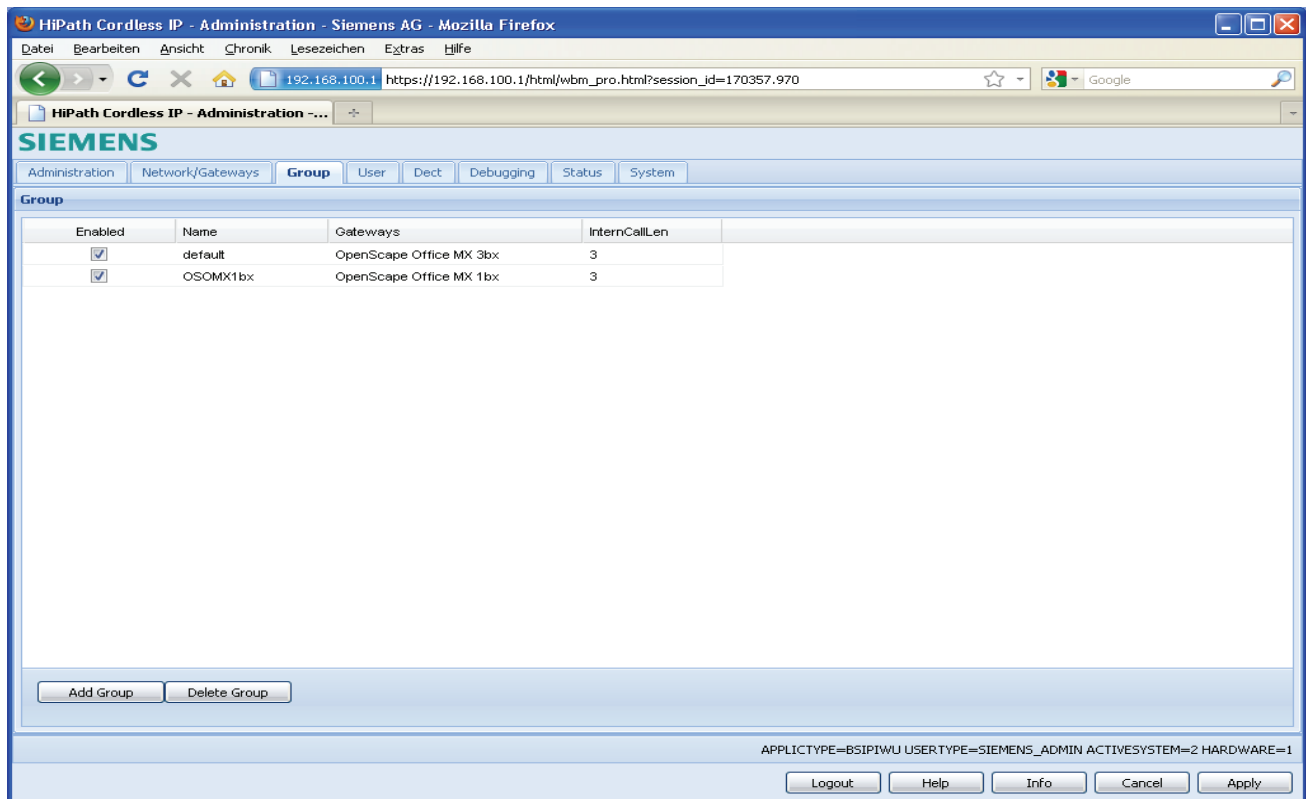
- • **Hint**: To add or delete a Group entry, the system services have to be stopped before. All changes will be activated after a restart of the system services.

1. To add a new Group entry, click on [**Add Group**].

   A new entry line with default values is appended, which have to be modified according to your System. The values have to be configured according your needs. The new entry line is either inserted above the selected Group or inserted at the top of the list if no Group is selected.

2. A selected Group entry may be deleted by clicking [**Delete Group**].

The columns of the configuration page have the following meaning:

Name

Enter a descriptive name for the Group (e.g the name of the corresponding gateway). This will be displayed in the dropdown box for the available Groups when configuring the VoIP Users.

Enabled

When activating this element the selected Group is enabled and displayed in the dropdown box for the available Groups when configuring the VoIP Users.

Gateways

Select the assigned Gateway for this Group via the select box. Hereby the assignment between a specific User to a specific gateway (PBX) is configured.

InternCallLength

With this setting the maximum number of digits of the calling Party number for internal calls is configured. Calls with a larger number of digits are signalled as external calls at the handset. The default value is "3".

5.3.6 Users Configuration (IWU)

On the sub configuration pages below "VoIP Users" ("User", "Voip" and "Dect")
the individual users and their properties regarding "User" (general user
properties), "Voip" (registration via VoIP) and "Dect" can be configured.
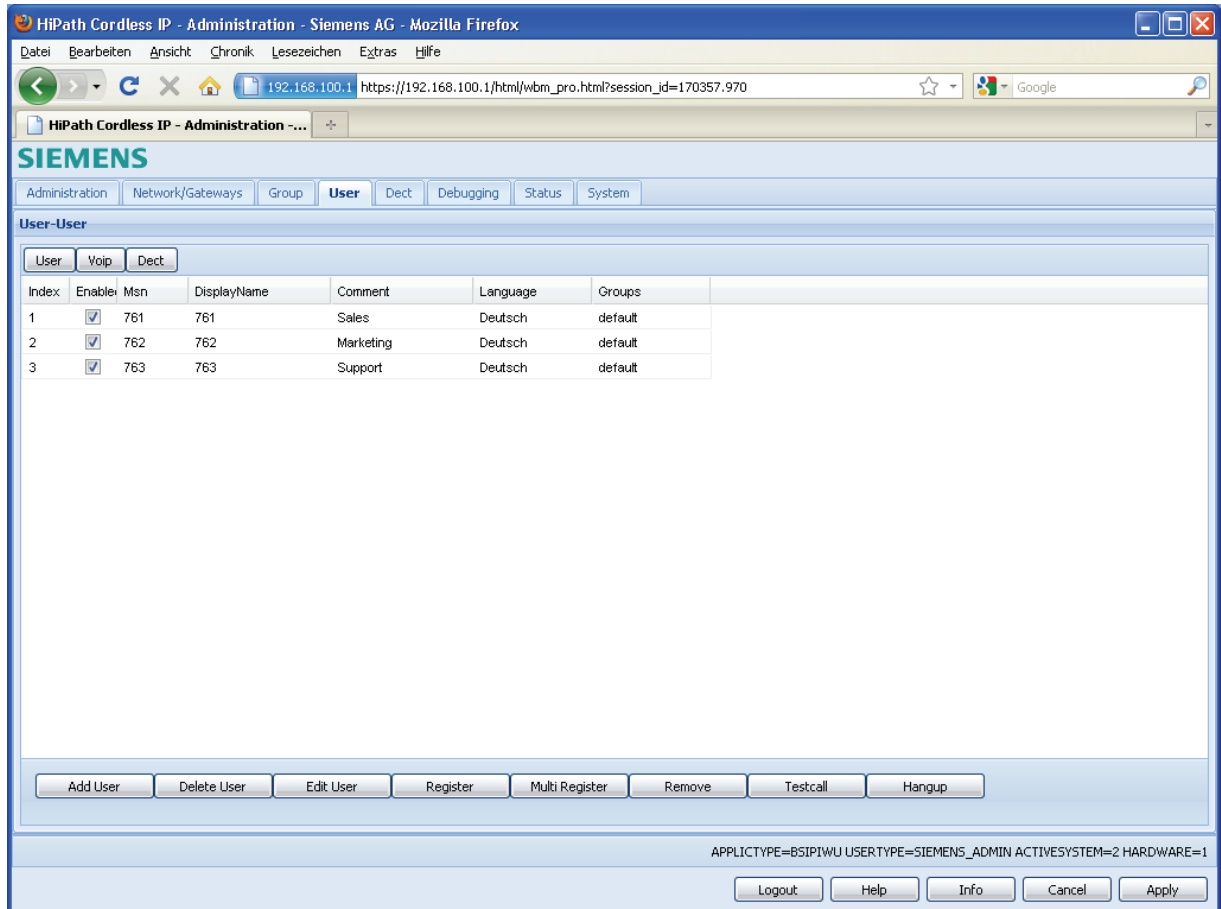
5.3.6.1 General user configuration

- **Hint**: Adding, editing and deleting of user entries is supported during running
  system services.

The buttons in the lower part of the page have the following functions:

[Add User]

To add a new user entry (even during running system services), click on [**Add
User**].
A new entry with default values is appended. The values have to be modified
according to your system needs.
The new entry line is either inserted above the selected user or - if no user entry

is selected - inserted at the end of the list.
If a group with name "default" is available and enabled, a new user entry is automatically assigned to group "default".

[Delete User]

A selected user entry may be deleted by clicking [**Delete User**], even during running system services if the user has no active call established.

Hint: The functionality [Delete user] does not remove the registration of the handset. It only removes the user entry from the WBM configuration. Therefore if you delete an user entry, the already existing DECT registration will create an "Auto entry" later (for details refer to chapter 5.3.6.4.1, "Auto Entry users".

[Edit User]

To enable the configuration of User settings during running system services, there is a special functionality ([Edit user]) available. To modify an existing user entry, select a user row and click on [Edit user] to change the values.

Selection of user entry prior to [Edit User]

Index	Enable	Msn	DisplayName	Comment	Language	Groups
1	✓	761	761	Sales	Deutsch	default
2	✓	762	762	Marketing	Deutsch	default
3	✓	763	763	Support	Deutsch	default

Selection of user entry after [Edit User]

Index	Enable	Msn	DisplayName	Comment	Language	Groups
1	✓	761	761	Sales	Deutsch	default
2	✓	762	762	Marketing	Deutsch	default
3	✓	763	763	Support	Deutsch	default

The user is locked until you press [Apply] to submit or press [Cancel] to discard the changes.

[Register]

The DECT registration process for a selected User is started by clicking on button [Register].

The registration mode will be activated for a certain period of time. At the handset of the User, the registration has to be started and the PIN number (as configured in chapter 5.3.7.3, "Configuration Page "Dect - ARI"") has to be entered when requested.

- **Note:** Restart the registration process if you did not succeed registering your handset in the provided period of time. The time is limited to avoid foreign handsets registering.

[Multi register]

The Multi register process eases the process of creating and registering a large amount of users.

To start the Multi Register process, at least one user entry (with start values) has to be configured manually. This entry serves as a template for the creation of further users during the Multi register process.

Select an existing, enabled User entry (this serves as the template user).

After clicking on [Multi register] a handset may be registered directly. After successful registering of the handset, a user entry with the IPUI of the handset is automatically created. The user values are automatically incremented from the last created user.

A new handset may be directly registered afterwards. This process may be repeated several times.
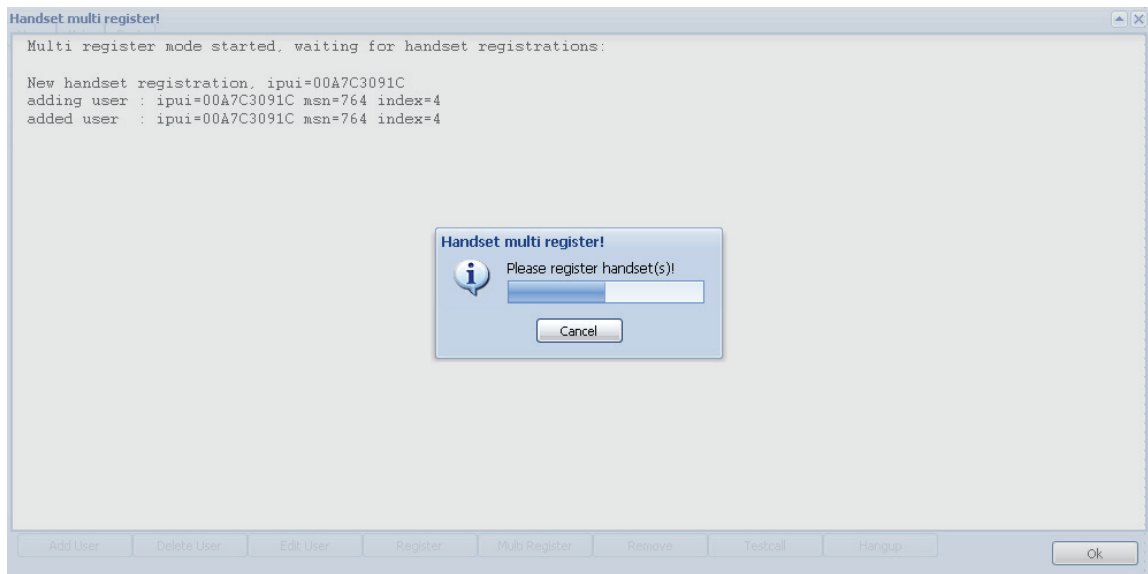
The Multi Register process may be stopped by using the [CANCEL] button.

Detail regarding the Multi register process may be found in chapter 5.4.2.3, "Multi-Register (Bulk Registering) of Handsets".

Remove

To remove the DECT registration of the handset for the selected User (Deregistering the handset), the button [Remove] has to be activated.

TestCall

This option performs a test call to the handset. The handset of the selected User must start ringing (if already registered). The call may be accepted at the handset (but no speech connection will be established) or the test call may be terminated by clicking on button [OK].
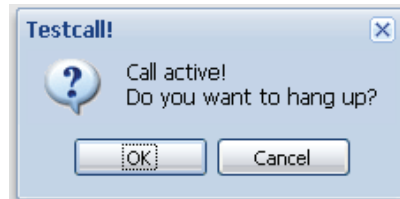
Hangup

An active Test Call may be terminated by clicking on using this button.

5.3.6.2 Configuration Page "User - User"

On this page the VoIP parameters for the Users are configured.

Index	Enabled	Msn	DisplayName	Comment	Language	Groups
1	☑	761	761	Sales	Deutsch	default
2	☑	762	762	Marketing	Deutsch	default
3	☑	763	763	Support	Deutsch	default

The columns of the configuration table have the following meaning:

Index

Current number of the User entry. This value is automatically incremented by the WBM.

Enabled

When activating this element, the selected User is enabled at the IWU.

MSN

The "MSN" has to correspond to the Subscriber Number of the User at the PBX (usually the "User Name" in the PBX). The MSN is internally used by the IWU to identify the users particularly for a PBX where the user registration ("UserNumber") is realized by a name instead of a number.

DisplayName

The handsets will display this value in their idle display. The activation of the DisplayName at the handset is initiated by an outgoing or incoming call.
There is neither an activation of the DisplayName due to a Power cycle of the handset nor to a roaming process.

The DisplayName at the handset is limited to a maximum of 10 Characters.

• **Important note:** Don't use characters others than 0-9, a-z, A-Z, "-" "_" for the DisplayName configuration. Other characters may prevent that the DisplayName is diplayed correctly.

Comment

The field "Comment" serves only as a reference for the system administrator of the IWU. It may contain for example the type of the Handset, the full name of the belonging user or the name of the department if the Handset is not associated directly to a person.

This field has no influence on the functionality of the WBM.

Language

The language used for display messages of the handset is selected here.

Groups

Choose a Group (and therefore an associated VoIP gateway) from the dropdown box to which the user is associated to.

5.3.6.3 Configuration Page "User - VoiP"

On this page the parameters for the SIP registration of the User at the PBX and the assignment of the subscriber numbers can be configured.

Index	Enable	Msn	DisplayName	Comment	UserName	AuthName	Password	G72
1	✓	761	761	Sales	761	761	1234	☐
2	✓	762	762	Marketing	762	762	2345	☐
3	✓	763	763	Support	763	763	3456	☐

(User-Voip: tabs User, Voip, Dect)

The columns of the configuration page have the following meaning:

- **Note:** The columns "Index", "Enabled", "Msn", "DisplayName" and "Comment" are repeated on all sub pages. A description of these parameters can be found in the previous chapter 5.3.6.2, "Configuration Page "User - User"".

Details regarding the correlation between the values used in the PBX configuration and in WBM may be found in the chapter for the used PBX at chapter 5.5, "Configuration Hints for PBXs".

UserName

Assign a User Name which is used for the registration at the PBX. This may be a name or a number depending on the PBX or the provider. For the supported gateways only numbers are allowed.

AuthName

The authentication Name is necessary if a PBX requires authentication of the user (Digest authentication). In case of digest authentication, the AuthName and Password are sent to the PBX as part of the registration process.

Password

Here the password is configured which is required (together with the "AuthName") if the PBX requires digest authentication.

G729

The usage of low bandwith codec G729 is intended for devices which are connected to the PBX via low bandwith lines (DSL) e.g. for home office users using a SIP phone (e.g OpenStage). Therefore bandwith is an issue for such scenarios.
Inside the LAN efficient bandwith should not be an issue; therefore codec G711 should generally be used. In this scenario there should be no need to configure

G729 in the codec list of the PBXs "Gateway - Codec" configuration page. Activating the codec G729 at the handset changes the codec list from G711A, G711U to G729ab; G711A, G711U.

Details regarding G.729 may be found in chapter 5.4.1.5, "Codec G.729".

5.3.6.4 Configuration Page "User - Dect"

This page contains the user configuration for DECT functions.

Index	Enabled	Msn	DisplayName	Comment	PnCap	Ipui
1	✓	761	761	Sales	✓	000542D1AF
2	✓	762	762	Marketing	✓	00BA99B1F6
3	✓	763	763	Support	✓	00BF382BAB

• **Note:** The columns "Index", "Enabled", "Msn", "DisplayName" and "Comment" are repeated on all sub pages. A description of these parameters can be found in chapter 5.3.6.2, "Configuration Page "User - User"".

Ipui

The IPUI (International Portable User Identity) of the Handset of the User is automatically recorded during the registration process.

5.3.6.4.1 Auto Entry users

The WBM may contain specific "auto entry" users under following conditions:

A handset has a valid registration at the IWU (acc. the System ARI), but no corresponding user can be found which contains the IPUI of the handset. In this case an auto entry user is added by the IWU.

Index	Enabled	Msn	DisplayName	Comment	PnCap	Ipui
1	✓	761	761	Sales	✓	000542D1AF
2	✓	762	762	Marketing	✓	00BA99B1F6
3	✓	763	763	Support	✓	00BF382BAB
4	☐	999	00A7C3091C	auto entry	✓	00A7C3091C

This auto entry user is displayed and treated as a normal user. Therefore it may be configured normally with the difference that no DECT registration process is needed for this user (since the handset is already registered at the handset).

• **Hint:** The auto entry user is additionally displayed on WBM page "Status - Calls Dect".

5.3.7 Dect Configuration (IWU)

On the main configuration page "Dect" the Base Stations are configured. This page contains the sub configuration pages "Device",""Sync", "ARI", and , "About".

There are further sub-pages available in WBM mode Siemens Admin.

5.3.7.1 Configuration Page "Dect - Base"

On this page the properties of the Base Station connections are configured. The columns of the configuration table have the following meaning:

Index

Index number of the DECT module (BSIP), automatically assigned by the WBM.

Enabled

By activating this option this Base Station is enabled at the BSIP-IWU.

• **Hints:**

The BSIP-IWU displays a maximum of 12 modules, whereby maximal 10 modules may be enabled.

The Server-IWU displays a maximum of 100 modules, whereby maximal 60 modules may be enabled.

Name

A unique name for the Base Station can be configured here (e.g. location where the BSIP is installed later). This name serves only for internal configuration purposes.

NumOfChannel

Number of voice channels of the Base Station in conjunction with the IWU. The maximum value is "10". If less than "10" parallel voice channels shall be supported, a smaller value may be configured here. The default value is "10".

IpAddr Module

The IP address of choice for the Base Station in the IP-DECT network is entered here. Please take care that the "IpAddr Module" address has to be unique and is in the same subnet as the IP address of the InterWorking Unit ("Server Ip").
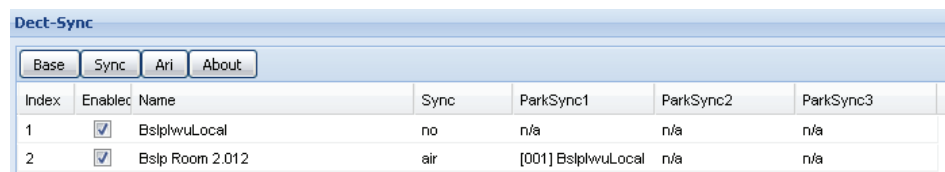
Please not that the IP address of the Base Station is transmitted to the Base Station after a [UDP Set] (see chapter 5.3.7, "Dect Configuration (IWU)").

MAC Addr

In this field the ethernet MAC address of the Base Station is displayed as it is found during a "Scan". It cannot be changed.

5.3.7.2 Configuration Page "Dect - Sync"

On this configuration page the synchronization of the Base Stations is configured.

Index	Enabled	Name	Sync	ParkSync1	ParkSync2	ParkSync3
1	✓	BslpIwuLocal	no	n/a	n/a	n/a
2	✓	Bslp Room 2.012	air	[001] BslpIwuLocal	n/a	n/a

The columns of the configuration page have the following meaning:

• Note: The columns "Enabled" and "Name" are repeated on all sub pages. A description of these values can be found in chapter 5.3.7.1, "Configuration Page "Dect - Base"".

"Sync" (Default value: "air")

Here you can configure the type of synchronization of the Base Station with a dropdown box.

The following settings are possible:

- "**no**": No synchronization of the Base Station. This may be configured if no "seamless handover" is needed or if this BSIP serves as the "Sync Master" for air synchronization which is the topmost synchronization source.

- "**air**": Default Synchronization of activated Base Stations over air, i.e. directly via DECT, but with additional Status information by the IWU.
  This method occupies - depending on the Beacon configuration - one or more available timeslots (which cannot be used for telephony), but it allows the seamless handover between the radio areas of synchronized Base Stations. The Base Station to be synchronized to must be an activated Base Station at the IWU.

- "**air ext**": Non-Default Synchronization of Base Stations over air, i.e. directly via DECT, but without additional Status information by the IWU.
  This method occupies - depending on the Beacon configuration - one or more available timeslots (which cannot be used for telephony), but it allows the seamless handover between the radio areas of synchronized active Base Stations.
  The Base Station to be synchronized to must be a Base Station configured at the IWU, but it need **not** be activated.
  Alternatively a Base Station may also be synchronized to another Base Station that is NOT configured at the IWU (e.g. Base Stations of other manufacturers).
  If the PARK of the external Base Station is known, it may be entered as "PARK Default" of the Base Station to be synchronized on the page "Ari". For the external Base Station a "Dummy" module has to be configured.
  Please notice that this may result in problems regarding the so called "Beacon Announcement" which may lead to frequent losses of synchronization.
  To minimize this problem an (internal) Base Station may be used as synchronization Base Station. Therefore you have to configure "0" channels (page "DECT - Device", entry "NumOfChannel"). No voice connections can be established via this Base Station.

- "**1588 master**": Configures the Base station to use Ethernet Synchronization over Ethernet (acc IEEE 1588) as Sync master (Clock master).
  Only one BSIP may be configured as "1588 master".
  A BSIP-IWU may not be configured as "1588 master".

- "**1588 slave**": Configures the Base station to use Ethernet Synchronization over Ethernet (acc IEEE 1588) as Sync Slave (Clock Slave).

"ParkSync" (3 columns)

- **Hint:** This option is only functional for BSIP which are synchronized via air (Sync option "air"). For Ethernet synchronized BSIP this option is without function.

You can choose a Base Station resp. DECT module from the select box on which the selected Base Station shall synchronize to (synchronization master). The Base Station will first try to synchronize to the Base Station in the leftmost "ParkSync" column. If this is not successful or if the synchronization gets lost while in operation, the Base Station will try to synchronize to the Base Station in the middle "ParkSync" column and finally to the rightmost column.
Only when the synchronization to all 3 entered Base Stations is not successful, a synchronized operation and therefore a seamless handover will no longer be possible.

Normally synchronization over air should be reduced to only one ParkSync (ParkSync1). If further BSIP are configured as ParkSync2 and ParkSync3 which have a low RSSI level of the received sync signal, this may lead to counterproductive system behaviour. In no case a fallback synchronization (ParkSync2 or ParkSync3) to a BSIP which is physically located behind a BSIP which is already configured as ParkSync1.

Please keep in mind, that the current BSIP may be selected in the dropdown menu. Since this would lead to a sync recursion, the local BSIP may not be configured as its own ParkSync.

- **Important note**: If a BSIP which is configured as Sync Slave looses synchronization, it tries to resynchronize to its configured synchronization Master Base Station (ParkSync). This process can not start until the last call at the Sync Slave BSIP is released and no other calls are active.

Further information regarding the Synchronization may be found in the following chapters:

Synchronization over air:

chapter 5.1.4, "Synchronization over air concept"

Synchronization over Ethernet:

chapter 5.1.5, "Synchronization via Ethernet (acc. IEEE 1588)"

5.3.7.3 Configuration Page "Dect - ARI"

On this configuration page the access rights (ARI - Access Right Identity) for the individual Base Stations as seen from the Handsets are configured.

The columns of the configuration page have the following meaning:

• Note: The columns "Enabled" and "Name" are repeated on all sub pages. A description of these can be found in chapter 5.3.7.1, "Configuration Page "Dect - Base"".)

RPN

When operating the Base Station stand alone and unsynchronized "0" (default value) has to be entered as RPN ("Radio Fixed Part Number").

For the setup of a network of synchronized DECT Base Stations this number is used for a handset to differentiate between the Base Stations for the seamless handover and it therefore has to be unique in the DECT network.

For DECT Base Stations with an ARI class A, the values 1 to 7 are allowed to differentiate between up to 7 Base Stations.

For DECT Base Stations with an ARI class B the values 1 to 255 are allowed to differentiate up to 255 Base Stations.

Cipher (only available in Siemens Admin mode)

By activating the ciphering feature, the communication between the handset and the configured base station is encrypted.

The setting is automatically applied to all base stations to the same value. The default value is enabled.

• **Hint:** The ciphering method uses the "System Pin" to cipher the DECT speech connections of the handsets on air. The "System Pin" is transmitted to the handset during the registration process. If the "System Pin" is changed later, this will lead to disturbed voice connections. In this case, the handsets have to be reregistered at the IWU.

5.3.7.4 Configuration Page "Dect - About"

This configuration page is only for information purposes on the created DECT configuration.

Click on [**Scan**] to update all values.

Index	Enable	Name	Type	Basestation:	Version	PartInfo1	PartInfo2	IpAddr Module	IpAddr Server	Server Port	Mac Addr
1	☑	BsIpIwuLocal	BsIpLocal	000000000	V3.32.14 Jan 20 2011 16:24:11	n/a	n/a	192.168.123.222	192.168.123.111	10500	00-00-00-00-00-00
2	☑	BsIp Room 2.012	BsIp	738479248	w3.32.14 Jan 20 2011 16:24:51 5	V3.32.14	V3.32.14 Active	192.168.10.2	192.168.10.1	10500	00-1a-e8-21-b0-73

The columns of the configuration page have the following meaning (only display):

• **Note:** The columns "Enabled" and "Name" are repeated on all sub pages. A description of these can be found in chapter 5.3.7.1, "Configuration Page "Dect - Base"".)

Type

Displays the type of the Base Station: "BsipLocal" for a BSIP-IWU or "BsIp" for a BSIP-Only.

BasestationSerialNr."

Displays the serial number of the Base Station as read with "Scan".

Version

Displays the version number and the version date of the current Firmware running on the active partition as well as the hardware revision of the BSIP as read with "Scan".

PartInfo1

Displays the version number of the firmware running on partition1 of the belonging BSIP-Only as read by a "Scan". Additionally, the label "Active" indicates, that this is the active partition of the BSIP.
For a BSIP-IWU (Type="BsIpLocal") this information may be derived from page Administration > "Version System 1" resp. "Version System 2".

PartInfo2

Displays the version number of the firmware running on partition2 of the belonging BSIP-Only as read by a "Scan". Additionally, the label "Active" indicates, that this is the active partition of the BSIP.
For a BSIP-IWU (Type="BsIpLocal") this information may be derived from page Administration > "Version System 1" resp. "Version System 2".

IpAddr Module

Displays the current IP address of a BSIP-Only , as read with "Scan".

- **Hint:** If this Ip address differs from the configured IP address (IpAddr Module)on page DECT-Base, a SYNC process has to be established, which transfers the settings of the BSIP configured at the IWU towards the BSIP.

IpAddr Server

Displays the IP address of the DECT Server IP (DECT network) read with "Scan".

- **Hint:** If this IP address differs from the configured Server IP (see page DECT) , a SYNC process has to be established, which transfers the settings of the BSIP configured at the IWU towards the BSIP.

Server Port Broad
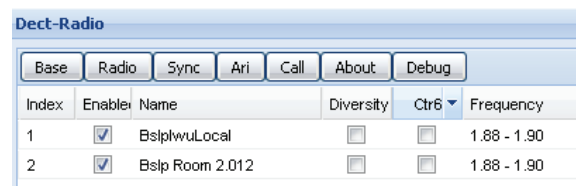
Displays the IP port of the BSIP-Only on which the BSIP-Only is communicating with the IWU (see option "ListenPort" on WBM page "Dect") as read from the Base Station with "Scan".

Mac Addr

Displays the MAC address of the BSIP as read from the Base Station with "Scan".

5.3.7.5 Configuration Page "Dect - Radio" (Advanced mode)

This page is only displayed in Siemens Admin mode at the WBM.

The columns of the configuration page have the following meaning:

Diversity

If this option is enabled, the antenna diversity feature for the selected BSIP is activated.

Ctr6

This option is exclusively needed for specific tests according CTR6. After activation of this feature, specified test cases may be initiated.

This option must not be activated during normal productivity operation of the HPCIP system.

Frequency

Selects the frequency of the DECT the BSIP is working with.
Standard setting: "1.88-1.90".

5.3.7.6 Configuration Page "Dect - Call" (Advanced mode)

This page is only displayed in Siemens Admin mode at the WBM.

NumOfChannel

In SiemensAdmin mode the configuration for number of channels is configured at this sub-page. In Normal mode the configuration may be found at configuration page "Dect - Base"
The standard value is 10.

Jitter

In SiemensAdmin mode the jitter buffers for the Dect Module may be configured here. Don't change the value from its default.

5.3.7.7 Configuration Page "Dect - Debug" (Advanced mode)

This page is only displayed in Siemens Admin mode at the WBM.

On the sub page "Debug" various logging and debugging functions may be activated for the individual DECT modules. Based on these functions potential problems in the DECT section may be investigated. For the analysis of the Log files profound knowledge of the DECT technologies is essential. Therefore debugging is intended primarily for our support staff.

• **Note:** Please note that depending on the activated Logging configuration big amounts of data may be produced which may have negative influence on the performance of the IWU Software and the System. Therefore you should only activate Logging functions when requested by a support engineer.

The columns of the configuration page have the following meaning:

• **Note:** The columns "Index", "Enabled" and "Name" are repeated on all sub pages. A description of these can be found in chapter 5.3.7.1, "Configuration Page "Dect - Base"".

Debug Disable (Default value: Deactivated)

When activating this entry the Logging functionality for the active DECT module is disabled, independent of the configured Debug level.

Debug Lvl (Default value: "0x00000000")

Debug level of the selected entry. The value may be entered directly as a hexadecimal value.

5.3.7.8 General DECT configuration

The configuration page "Dect" is divided into two parts.

In the table view at the top, all BSIP modules are configured.

At the bottom of the page, the general DECT configuration of the DECT Network is done.

- **Hint:** All changes will be activated after a reboot of the BSIP.

5.3.7.8.1 Adding, Deleting and Scanning

[Delete Module]

By selecting a base station and clicking on [Delete Module], the selected Base Station entry is deleted.

[Scan]

This functionality (Scan) initiates a Seek or Scan of the network for all attached BSIPs using an ip broadcast mechanism.

All BSIP-Only are answering and sending their current configuration information (mainly its own IP address, the IP address and listen port of the IWU, its name and VPN configuration) to the IWU where it is displayed. For newly scanned BSIPs to which no configuration (according the MAC address) is assigned, a new entry is automatically added.

- **Hint:** The values stored in the configuration of the WBM are overwritten with those found by the SCAN of the corresponding BSIP. This fact has to be considered especially for the configuration of the name of the BSIP. First Scan the BSIP, change the name and afterward initiate a Sync.

Depending on the VLAN configuration of IP Infrastructure and IP Dect network, the BSIP-Only are only found if they are attached to the appropriate network segment. For details refer to option "VLAN Id" of the Voip (Infrastructure network) at chapter 5.3.4.2, "Network configuration" and of the DECT network at chapter 5.3.7.8.2, "General configuration options".

- **Hint:** If communication specific options of a BSIP are changed at the IWU, a [Sync] process has to be established. Otherwise the formerly active IP address of the BSIP will be still displayed.

If newly added BSIP are not found using [SCAN], repeat the [SCAN] process with stopped system services. Otherwise take note of the hints described at chapter 5.6.1.1, "BSIP-Only is not found using "Scan"".

[Sync]

This functionality (Sync) initiates the transmission of the relevant configuration data (mainly its own IP address, the IP address and listen port of the IWU, its name and VPN configuration) from the IWU to all enabled BSIP-Only.
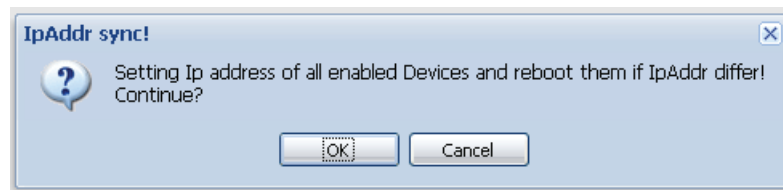
5.3.7.8.2 General configuration options

Server Ip

This field contains the IP address of the IWU inside the DECT network. This IP address is used for communication between the IWU and all BSIP-Only.

The factory default Ip address is 192.168.1.1, which may not be saved inside the configuration of the IWU.

- **Hint:** The configured IP address may not be located inside the network of the configure Voip (Infrastructure) Ip address.

For detail refer to chapter 5.4.2.1, "Free IP Addressing".

Network Mask

By default, a netmask of 255.255.255.0 (24 bit) is configured for the DECT network. Please keep in mind, that using another netmask than 255.255.0.0 will prevent BSIP-ONLY running with firmware V1R1 being found in SCAN.

For detail refer to chapters

chapter 5.4.2.1, "Free IP Addressing" as well as
chapter 5.4.2.2, "Adding new BSIP".

Listen Port

This field defines the IP port on which the communication between the BSIP-IWU and BSIP-Only is established. The default value is 10500.

IWU as GW

This option is only intended to access the BSIP-Only when different VLANS and/or VPNs are configured. This option activates the routing functionality between the VoIP (Infrastructure) network and the DECT network on the IWU.

- **Hint:** Using the BSIP-IWU as a router influences the system (e.g. system load for encryption) and may lead to unpredictable system behavior.

Use this option only in case where other IP access is not available, e.g.

- SSH access to BSIP-Only

- Access to WBM of BSIP-Only

- Local Firmware update of BSIP-Only

Therefore, you have to add a route at the maintenance PC (Windows XP):

Example:

IP of IWU is 192.52.109.83, IP-DECT network is 192.168.201.0/255.255.255.0

To permanently add a route at the administration PC, type in at a command windows:

route -p add 192.168.201.0 MASK 255.255.255.0 192.52.109.83

- **Hint:** If you have formerly configured an IP address at the maintenance PC within the DECT network, don't forget to delete this address at the XP PC before adding the route.

SystemAri

In this field the System ARI (DECT ID) which has to be unique at each DECT system has to be configured. The SystemAri is provided by the system implementor. Supported System Ari classes are Class A and Class B Ari.

- **Hint:** All handset registrations are bound to a specific System ARI. If the System ARI is changed, all handsets loose their registration at the IWU. To achieve system functionality, the handsets have to be registered again at the IWU.

SystemPIN

The "PIN" is a 8-digit number and it is needed for the registration of Handsets. It is preconfigured with "00000000" and may be configured systemwide here.

- **Hint:** The ciphering method uses the "System Pin" to cipher the speech connections of the handsets on air. The "System Pin" is transmitted to the handset during the registration process. If the "System Pin" is changed later, this will lead to disturbed voice connections. In this case, the handsets have to be reregistered at the IWU.

No new modules on scan (only in advanced config. Mode)

This new function is mainly intended for testing purposes in a lab environment with a lot of different Base stations for different HPCIP systems. Normally, all modules are scanned and each entry is added at the DECT modules table. Activating this option, the [SCAN] functionality doesn't add new entries of Base station into the table.

VPN Enable

This option enables the encryption of data communication (signalling and voice data) between the IWU and all BSIP-Only. Encryption is realised by using an ipsec connection in transport mode using static keys.

- **Hint:** Some system relevant functions (e.g. SCAN and SYNC) are transmitted unencrypted.

VLAN Id

The corresponding VLAN Id (according IEEE 802.1q) for the DECT network is configured here.

- **Important note:** Regardless of the value configured here, the BSIP-Only is not able to handle tagged Ethernet packets. This is due to the fact that a BSIP-Only has no local console access (as compared to a standard cable based SIP phone) and therefore may not be accessible anymore if VLAN is

not configured correctly. For this reason, the Switchport - at which a BSIP-Only is attached to - has to be configured untagged and assigned the VLAN Id configured here.

This does not apply to a BSIP-IWU or a Server-IWU. The BSIP-IWU and Server-IWU are able to handle tagged Ethernet packets. For details refer to option "Vlan Id" of the Infrastructure network at chapter 5.3.4.2, "Network configuration".

All Ethernet frames towards the VoIP (Infrastructure) network between the IWU and the Ethernet switch are tagged with the configured VLAN Id configured for the Infrastructure network (option VLAN Id" at page Network/Gateways).

All Ethernet frames towards the DECT network between the IWU and the Ethernet switch are tagged with the configured VLAN Id configured for the DECT network (option "VLAN Id" at page DECT - this option).

Please take account of the correlating VLAN configuration of the VoIP (Infrastructure) network at chapter 5.3.4.2, "Network configuration".

5.3.8 Debugging Configuration (IWU)

This page is only displayed with Siemens Admin mode at the WBM.

On the page "Debugging" various Logging and Debugging functions may be activated. Based on these functions potential problems regarding DECT, VoIP or interworking functionality maybe isolated. For the analysis of the Log files profound knowledge of VoIP and DECT connections is essential. Therefore they are intended primarily for our support staff.

The sub pages "**Server**", "**Iwu**" "**Voip**" and "**DLL**"differentiate the various parts of the Software for which Debugging may be activated. They differentiate the names of the Software levels and the according Log file names. You will get more detailed information from our support engineer when the activation of a Debug level is requested.

- **Note:** Please note that depending on the activated Logging configuration big amounts of data may be produced which may have negative influence on the performance of the IWU Software and the System. Therefore you should only activate Logging functions when requested by a support engineer.

The options of the table have the following meaning:

Disable (Default value: Deactivated)

When activating this entry the logging functionality for the selected entry is disabled, independent of the configured Debug level.

Name (fixed)

Preconfigured descriptive name of the Software level for which the Debug level is valid. You will get more detailed information from our support engineer when the activation of a Debug level is requested.

Level (Default value: "0x00000000")

Debug level of the selected entry. The value may be entered directly hexadecimal or via the checkboxes on the right.

The options of the lower part of the configuration page have the following meaning:

Console (Checkbox and entry)

By activating this entry the Debugging functionality via the Console application is enabled.

The entry contains the associated UDP port number for Remote Debugging.

Logfile

By activating this entry the Debug output is written to the associated Log files.

You may choose exclusively between Option Logfile or Syslog

Logfilename

This entry shows the name format of the Log file created.

Syslog

By activating this entry the Debug output is written to the associated Sylog server.

You may choose exclusively between Option Logfile or Syslog.

- **Hint:** IWU debugging messages are logged to a configurable syslog daemon with Facility="LOCAL1" and SEVERTIY Level="ALERT".

Start Syslog

If option "Syslog" is enabled activating this option starts a process which sends the syslog messages to the syslog server configured by option "Syslog Server Ip".

If this option is deactivated, no syslog messages are sent to the syslog server.

Syslog Server IP

The IP address of the syslog server (to which syslog output will be sent) is configured here.

Logfile Size Total

Displays the limit of the the maximum allocated disk space in bytes for all log files (stored in the "Log Path") here. A process checks periodically if the total size is reached. If the limit is reached, the oldest Log Files are deleted to free up disk space.

Logfile Size

Displays the limit of the the maximum file size in bytes of a single logfile here. As soon as this size is reached the log output is continued in a new file.

LogPath All

Displays the LogPath the files are stored on the BSIP.

Download logfiles

With this Button all logfiles of the BSIP may be downloaded and stored on the file system of the maintenance PC.

1. After clicking on the button [**Download logfiles**], an browser based file open dialog will be displayed immediately.
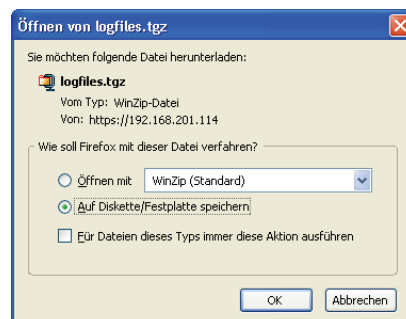
2. You have to select the store method of the dialog, click on button **[OK]** and select from the following "save as" dialog a folder to store the configuration files on the maintenance PC or a directory available via the network (default: "logfiles.tgz").
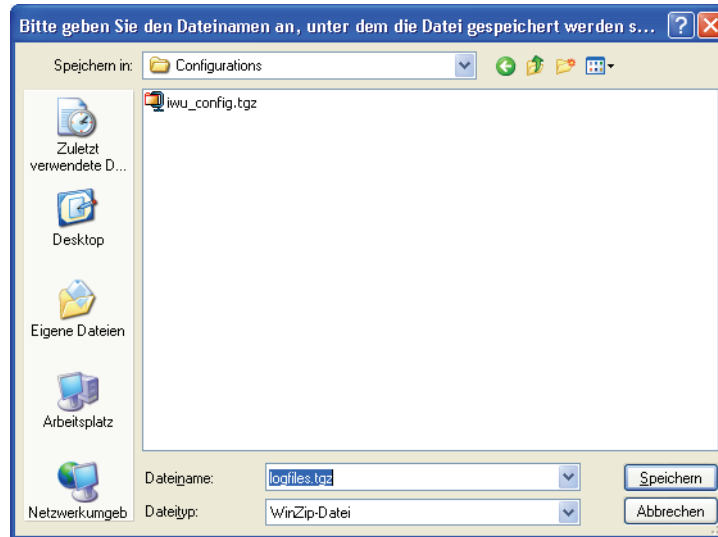
3. Save the configuration file using the default name "logfiles.tgz" or change it according your needs (Don't use blanks in the filename).

Clear logfiles

Use this function to clear the logfiles in the log directory.

Download Corefiles

Use this functionality to download coredump files which may have been created during a crash of the system processes.

If one of the main system processes of the IWU (Setup Application, Capiserver or InterWorking Unit) terminates contrary to expectations this will lead to loss of system functionality. The IWU has to be rebooted to gain system functionality again.

After reboot has finished, the diagnostic data (Corefiles) of the last crash may be downloaded by clicking on [Download Corefiles] and transmitted to the support team of the HPCIP system for analysis.

5.3.9 "Status" Configuration (IWU)

On the page "Status" of the Configuration Utility various status information may be displayed. It consists of several sub pages:

- On the first sub page (**[Modules 1]**) general information about the base stations is displayed.

- On the second sub page (**[Modules 2]**) enhanced information about the Base Stations is displayed.

- On the third sub page (**[Calls Dect]**) user specific DECT information are displayed.

- On the fourth sub page (**[RSSI]**) the current allocation of the DECT radio interface is displayed in a Table (RSSI Table).

5.3.9.1 General Status Information

The options at the lower part of page Status have the following meanings:

Options "RSSI", "Db", "Limit" and "Module" are described at chapter 5.3.9.5, "Configuration Page "Status - RSSI"".

hide disabled users

If this option is enabled, only entries for enabled user are shown.

active calls only

If this option is enabled, only entries of users with an active connection are shown.

Cycles (s)

If a numeric value different than "0" is configured, the display will automatically refresh after the configured number of seconds. After changing this value, the button [Refresh] has to be clicked.

• **Please note:** High frequency update rates (e.g. 1, 2 or 3 sec.) should be avoided.

Refresh / Stop

Manually refreshes the counters displayed.

After changing the value of option "Cycle (s)" unequal to 0, the automatic refresh will be active after clicking on [Refresh]. The caption of the [Refresh] button then changes to "Stop". After a reapply of button [Stop] the automatic refresh will stop and the caption of button [Stop] changes back to [Refresh].

Clear Statistics

Clears (resets) all counters to 0 after a confirmation dialog.

On the right side of the lower frame some options are located to select the time frame of the displayed values. The time frame is displayed in the fields "from:" and "to".

The format of the time frame is "Date [Event]" (e.g. "19.01.2011 07:13:11 cleared").

The following events are available:

• cleared state has been deleted by clicking on [Clear Statistics]

• inited state has been deleted by a System Update

• timediff state has been deleted by setting the system time

• timezone state has been deleted by changing the timezone

• restore state has been deleted by a configuration restore

- regular state is valid

The following date formats are used:

- "dd.mm.yyyy hh:mm:ss" is used for output of a specific date / time

- "now" Indicates that output is displayed up to the current point of time

from:

Displays the start of the time frame for the displayed values..

to:

Displays the end of time frame of the displayed values.

[Previous]

Selects the previous time frame of the status values (if available).

[Next]

Selects the next time frame of the status values (if available).

[Absolute]

Selects an absolute time frame of the status values (from the earliest available point of time up to now).

5.3.9.2 Configuration Page "Status - Modules 1"

Module	Name	Online	Sync	Carrier	Timeslc	Online last	Offline last	State 1588	Drift initial
1	BslplwuLocal	YES	YES	00	00	24.02.2011 08:00	N/A	5	-155
2	Bslp Room 2.012	YES	NO			24.02.2011 08:00	N/A	0	0

The columns of the table have the following meaning:

Module

This field contains the consecutive number of the BSIP 1.

Name

The name of the Base Station as read from the Base Station via "Scan".

Online

"Yes" if the selected Base Station is in state "Online"

"No" if the selected Base Station is in state "Offline"

- **Hint:** A Base Station is only functional, if its state is online. Therefore, the BSIP has to be synced, running the same firmware version on the same partition as the IWU and Ethernet and ip communication between the Server and the BSIP is established.

Sync

"Yes" if the selected Base Station is in "Sync" (synchronized), which means that this base station has synchronized to another base station. At the base Station which is not synchronized to another base (an exclusively Sync Master), the value is always "No".

Carrier

Displays the carrier number of the Synchronization channel the BSIP is synchronized to via air.
For synchronization via Ethernet, this field is empty.

Timeslot

Displays the timeslot number of the Synchronization channel the BSIP is synchronised to via air.
For synchronization via Ethernet, this field is empty.

.Online last

Displays the timestamp (date and time) at which a BSIP lastly changed its state to Online.

This time stamp is initially set when the system services are started. After this state, an "Online last" entry will be generated if the BSIP changes its state from Offline to Online.

Offline last

Displays the timestamp (date and time) at which a BSIP lastly changed its state to Offline. If the status changes to Offline, the "Online last" counter will be cleared.

Possible reasons for an Offline event are mainly Ethernet ip connectivity problems between the IWU and the BSIP-Only.

The following counters are only displayed for BSIP which are configured as 1588 Sync slaves.

- **Hint:** These counters are solely provided for analysis of possible Ethernet synchronization (acc. IEEE1588) issues and therefore are not described in detail.

Status-Modules1

| Modules1 | Modules2 | CallsDect | RSSI |

eslo	Online last	Offline last	State 1588	Drift initial	Delay min	Jitter avera	Time diff	Delay req r	Delay min r	Delay min r	Delay resp	Sync ind m	Limit1 reacl	Limit2 reacl	Limit3 reacl
	24.02.2011 08:00	N/A	5	-155	16260	135	60	0	0	0	1	0	1	0	0
	24.02.2011 08:00	N/A	0	0	0	0	0	0	0	0	0	0	0	0	0

State 1588

This counter displays the current state of the 1588 sync mechanism of a 1588 Sync Slave. (Standard state during runtime is "5" [In Sync]; Boot states are "2","3", "4").

Drift Initial

This counter displays the Initial Drift between the 1588 Sync Slave and its 1588 Sync Master.

The value is displayed in nano sec. per 100 msec.

Delay min

This counter displays the minimum sync delay (in nano sec.) of the current 1588 Sync Slave to its 1588 Sync Master.

This value corresponds to the one-way delay time of a 1588 Sync Slave to its 1588 Sync Master between all switch hops.

More number of switch hops between a 1588 Sync Slave and its 1588 Sync Master will increase this value.

Jitter average

This counter displays the average jitter (in nano sec.) of the current 1588 Sync Slave to its 1588 Sync Master.

Time diff

This counter displays the current time difference or offset (in nano sec.) of the current 1588 Sync Slave to its 1588 Sync Master.

Delay req retry

This counter displays how often an incomplete DELAY_REQ cycle was detected.

Delay min retry

This counter displays how often a retry to gather the absolute time difference was established.

Delay min new

This counter displays how often a retry to gather the absolute time difference with a new calculated Delay min window was established.

Delay resp miss

This counter displays how often a missing DELAY_RESP message was detected.

Sync ind miss

This counter displays how often a missing SYNC_IND message was detected.

Limit1 reached

This counter displays how often a short term absolute time difference in a range smaller than 1000 nano sec. was detected.

Limit2 reached

This counter displays how often a short term absolute time difference in a range between 1000 and 5000 nano sec was detected.

Limit3 reached

This counter displays how often a short term absolute time difference in a range between 5000 and 20000 nano sec. was detected. If this period was detected over a time period of longer than 50 seconds, the 1588 Slave will go OutOfSync and a resynchronization process for this BSIP will be initiated.

5.3.9.3 Configuration Page "Status - Modules 2"

Status-Modules2

Modules1		Modules2		CallsDect		RSSI								

Module	Name	Online	ISyncCnt	OnlineCnt	BootCnt	Outgoing call	Incoming calls	Intracell hand	Intercell hand	Roaming	Ovl 70	Ovl 100
1	BslpIwuLocal	YES	1	12	24	1	2	0	1	28	0	0
2	Bslp Room 2.(	YES	12	12	12	1	0	0	1	16	0	0

- **Hint:** The counter "OnlineCnt" and "BootCnt" are incremented by starting the system services, which reset the BBC on the BSIP and therefore are incremented by "1".

Module

This field contains the consecutive number of the BSIP.

Name

The name of the Base Station as read from the Base Station via "Scan".

Online

"Yes" if the selected Base Station is "Online", "No" if its "Offline".

ISyncCnt (In Sync Count)

This counter displays how often the Base Station did a resynchronization since the start of the system services.

OnlineCnt (Online Count)

Thsi counter displays how often a Online/Offline change has been detected since the start of the system services.

BootCnt (Boot Count)

This counter displays how often the Base Station was booted since the start of the system services.

Outgoing calls

This counter displays how often an outgoing connection (direction handset to BSIP to PBX) has been signalled.

Incoming calls

This counter displays how often an incoming connection (direction PBX to DECT to handset) has been signalled.
This counter is also incremented for calls where the connection was not successfully established.

Intracell handover

This counter displays how often a Intracell handover (handover of a DECT channel within the same DECT Base Station) was detected at the BSIP.

Intercell handover

This counter displays how often a Intercell handover (handover of a channel between different DECT Base Stations) was detected at the BSIP.

Roaming

This counter displays how often a roaming event (change of a Base Station without an active connection) was detected at the BSIP.

• **Hint:** Handover events (Intercell handover during an active call) are not considered by this counter. These events are handles by counter "Intercell handover".

Ovl 70

This counter displays how often the BSIP has allocated equal or more than 70 % of the available channels.

For a standard configuration of a BSIP with 10 calls (see configuration option "NumOfChannel" at chapter 5.3.7.1, "Configuration Page "Dect - Base"" per BSIP the counter is triggered if 7 calls are active on the DECT side.

Ovl 100

Zeigt an, wie oft die entsprechende Basisstation 100 % der verfügbaren Kanäle allokiert hat.

For a standard configuration of a BSIP with 10 calls (see configuration option "NumOfChannel" at chapter 5.3.7.1, "Configuration Page "Dect - Base"" per BSIP the counter is triggered if 10 calls are active on the DECT side

5.3.9.4 Configuration Page "Status - Calls Dect"

The columns of the table have the following meaning:

User

This field displays the "DisplayName" of the associated User.

Msn

This field displays the "MSN" of the associated user.

Voip states

This field displays the Voip state of the User ("No ras", "Ras up", "Ras down").

Ras changes

This counter displays the number of Voip state changes of the user (see Voip states).

RAS IP

This field displays the current IP address of the SIP server which was used for the last SIP message of the user.

Call states

This field displays the current Call state of the User ("Located on", "No location", "Calling out", "Alerting out", "Connected out", "Calling in", "Alerting in", "Connected in", "Switched off", "Removed").

Located

This field displays the number of the Base Station the User is located on.

Call located

This field displays the number of the Base Station on which the current/last call was located on.

Carrier

This field displays the Carrier number on which the connection for User "User" is active.

Timeslot

This field displays the Timeslot number on which the connection for User "User" is active.

Incoming calls

This counter displays the number of incoming connections (direction PBX -> BSIP -> handset) which have been signaled for the User.

Outgoing calls

This counter displays the number of outgoing connections (from direction handset -> BSIP -> PBX) which have been signaled for the User.

Intracell handover

This counter displays how often an Intracell handover (transfer of a channel within the same Base Station) was detected for the User.

Intercell handover

This counter displays how often an Intercell handover (transfer of a channel between different Base Stations) was detected for the User.

Roaming

This counter displays how often a roaming event (change of a Base Station without an active connection) was established for the current handset..

- **Hint:** Handover events (Intercell handover during an active call) are not considered by this counter. These events are handles by counter "Intercell handover".

5.3.9.5 Configuration Page "Status - RSSI"

SIEMENS

Timeslot	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9
Tx 00	+++	+++	+++	+++	+++	+++	+++	+++	+++	
Tx 01		-79	-77	-50	-79					
Tx 02	-63	sss	sss	sss	sss	sss	sss	sss	sss	sss
Tx 03										
Tx 04		bbb	bbb	bbb	bbb	bbb	bbb	bbb	bbb	bbb
Tx 05										
Tx 06	+++	+++	+++	+++	+++	+++	+++	+++	+++	
Tx 07	-61									
Tx 08	-84							-72		
Tx 09	-72	-47	-71							
Tx 10			-66							
Tx 11										
Rx 00	+++	+++	+++	+++	+++	+++	+++	+++	+++	-21
Rx 01					-66					
Rx 02					-77					

Modules1 Modules2 CallsDect RSSI

○ RSSI Limit: -85 □ hide disabled users Cycle (s): 0 from: 23.02.2011 11:12:56 timediff
● Db Module: [002] Bslp Room 2.012 □ active calls only Refresh to: now
Clear Statistics Previous Next Absolute

APPLICTYPE=BSIPIWU USERTYPE=SIEMENS_ADMIN ACTIVESYSTEM=2 HARDWARE=1

Logout Help Info Cancel Apply

On this page the table with the DECT RSSI values is displayed. The table has the following structure:

- **Lines (Tx 00 - Rx 11)**

  On these lines the timeslots Tx00 - Tx11 and Rx00 - Rx11 are displayed.

- **Columns (C0 … C9)**

  On these columns the carriers C0 - C9 are displayed.

Cell values:

"bbb"

"bbb" inside a line (timeslot) indicates that this is a timeslot with a beacon (sent signal).

One cell in the line shows the signal level (receive level) of the received value of the channel allocation of other DECT devices. This value shall be as small as possible.

"sss"

- **Hint:** This option is only applicable for air synchronization.

"sss" in a line (timeslot) indicates that this is a timeslot with a synchronization signal (received SYNC signal).

One cell in the line shows the carrier on which the sync signal is received on as well as the signal level (receive level) of the Sync signal. This value shall be as high as possible (-50 dB … -80 dB).

Important note: For accurate and stable synchronization over air a minimum signal strength of -75 dB (resp. 16 [RSSI]) should be achieved.

"+++"

"+++" in a line (timeslot) indicates that this is a Tx timeslot with a voice channel (unidirectional) signal (The timeslot number of the Rx channel is Tx Channel + 12).

One cell in a "Tx" line displays the value of the used Carrier for the voice channel.

One cell in a "Rx" line displays the receive level of the Base Station in relation to the active call.

"<value>"

Shows the current value (receive resp. send signal of the Rx resp. Tx timeslot) depending on the configuration of "RSSI", "Db" and "Limit".

Value ranges:

minimal value (corresponds to poor signal strength)-85 dB (resp. 9 [RSSI])

maximum value (corresponds to good signal strength)-50 dB (resp. 31 [RSSI])

Values outside a bbb, sss, or +++ line display the signal level (receive level) of other DECT devices. The number of values as well as their value itself shall be as small as possible.

The options at the lower part of the configuration page have the following meanings:

"RSSI"

The values displayed in the RSSI table are RSSI values.

"Db"

The values displayed in the RSSI table are Db values.

"Limit"

Here you can configure a minimum value. Only values greater (in the case of "Db" only values smaller) than "Limit" are displayed in the RSSI table.

Normally the following default values are used:

RSSI: "9"

Db: "-85"

"Module"

Here you may select the Base Station which values are displayed at the table.

5.3.10 "System" Configuration (IWU)

On the configuration page "System", both software processes of the IWU may be configured, started and stopped.

Click [Start] to start the enabled processes and [Stop] to stop them again. The current state of the services may be queried by clicking on [Refresh].

Activate "Service" for both entries if the services should start automatically at system start. Other modifications are usually not needed here.

The columns of the configuration page have the following meaning:

"Enabled"

Usually both processes are activated. This default configuration should only be changed for locating problems after consultation of the support team.

"Applic Name"

The Name of both IWU processes are displayed here.

"Status"

In this column the states of the IWU processes are displayed ("Stopped", "Started" or "Running").

Up since

Displays the time the service was started lastt

"Service"

Usually both services are activated which means that the corresponding process is started automatically after rebooting the BSIP.

5.3.11 "CLC" Configuration (only for Server-IWU)

If a Server based IWU (HPCIP-Server) is used, a specific license is needed. Without a valid license, the HPCIP System will be not functional.
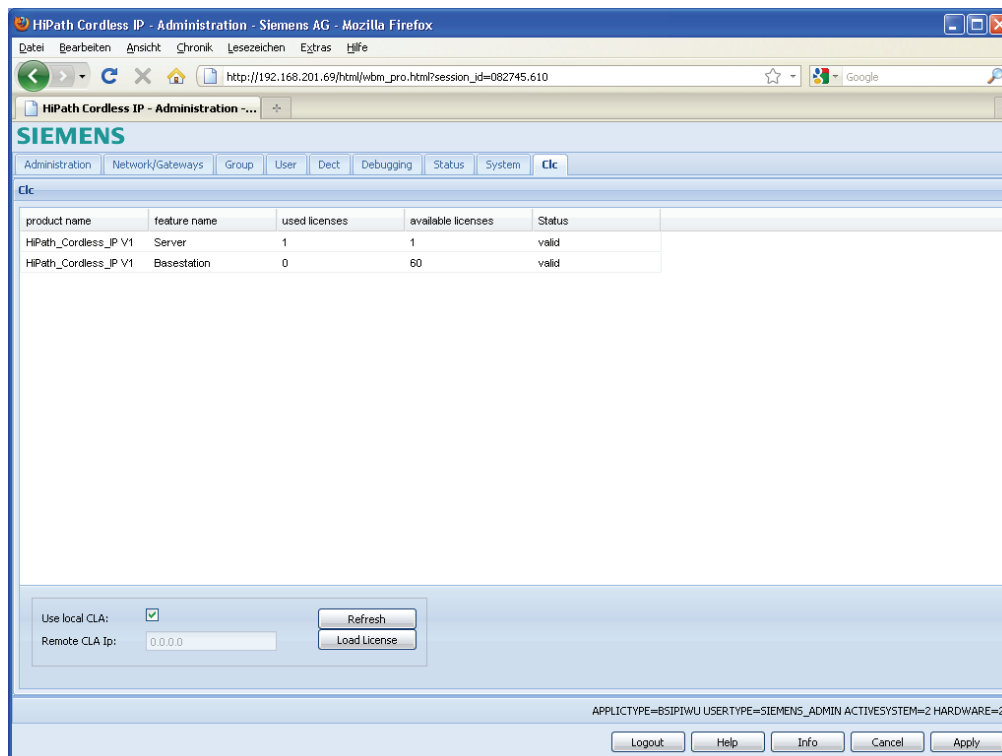
- **Hint:** The MAC address of the SERVER (HPCIP-SERVER) may be found in the output of "Version System" on WBM page "Administration".

The columns of the table have the following meaning:

product name

This column displays the product name of the license option (e.g. "HiPath_Cordless_IP V1").

feature name

This column displays the name of the license option (e.g. "Server" or "Basestation").

used licenses

This column displays the currently used number of license units of the corresponding license option.

available licenses

This column displays the currently available number of license units of the corresponding license option.

Status

This column displays the license state of the corresponding license option. Possible states are "failure", "grace period", "grace period, %d days left", "valid", "valid, %d days left", "failover".

The options in the lower part of the configuration page have the following meaning:

Use local CLA

If this option is enabled, the license file will be loaded and stored on the IWU.

If this option is disabled, a remote license server ("Remote CLA") may be configured as license server.

Remote CLA Ip:

If option "Use local CLA" is disabled, the IP address for the remote license server (from which the IWU gathers license information) may be configured here.

[Refresh]

A click of in on this button refreshes the display of all values.

[Load License]

If option "Use local CLA" is enabled, the license file may be uploaded via a file save dialog and stored locally on the IWU.

5.4 Configuration techniques and technologies

5.4.1 Technologies

5.4.1.1 SNMP

SNMP (Simple Network Management Protocol) is used by the HPCIP system mainly to detect overload situations of the system. These may be queried by a SNMP Server (SNMP MIB - Management Information Base) or may be signaled by the IWU (SNMP Trap).

The implementation uses SNMP version 2 with fixed ports. For the HPCIP system, a specific MIB file is available. The Name of the used MIB is "HPCIP-MIB".

The IWU provides besides SNMP values and tables (which may be queried with a SNMP manager) also SNMP traps which are signaled to a SNMP management system (which IP address has to be configured in the WBM of the IWU).

Since a lot of data has to be queried by the IWU for each SNMP request, this will lead to a high system load of the IWU (especially on a BSIP-IWU), a special mechanism was implemented to refresh the tables only if needed. Therefore, a specific SNMP value has to be queried by the SNMP management system to trigger the actualization of the SNMP tables by the IWU.

5.4.1.1.1 Implementation Details

The SNMP MIBs provide statistical data of the IWU (one table per day) to retrieve them by SNMP queries. A maximum of 14 statistical tables for the last 14 days are stored. Therefore one table holds the data for the current time period (current day), the other tables provide data for the last 13 days.

The naming conventions of the SNMP values according the OID (Object Identifier) is composed as follows:

The table with the current period of time is assigned to the relative OID .1, the table of the last day is assigned to the relative OID .2, the table of the day before yesterday is assigned to the relative OID .3 and so on.

5.4.1.1.2 SNMP MIB tree

The "Root-OID" is assigned to the OID 1.3.6.1.4.1.36378.

All MIBS ("BSIP_MIBS") are located inside the OID {Root-OID}.1.n

SNMP Table Definition

Value	Type	Description
From	Text	Date/time/reason of start of the current MIB table
To	Text	Date/time/reason of **stop** of the current MIB table
RPN	Text	RPN of the associated BSIP
MAC	Text	MAC address of the associated BSIP
Name	Text	Name of the associated BSIP
OVL70	Text	This counter indicates how often **70%** or more of the available channels of the associated BSIP had been occupied
OVL100	Text	This counter indicates how often **100%** of the available channels of the associated BSIP had been occupied
Roaming	Text	This counter indicates how often a roaming process (location event of a handset without an active connection) have been indicated at the associated BSIP. Hint: Handover events (Intercell handover during an active call) are not considered by this counter.

5.4.1.1.3 SNMP Trap Tree

All TRAPS ("BSIP_TRAPS") are located inside the OID {Root-OID}.2.n

SNMP trap definition

TR_BSIP_OnlineState ({Root-OID}.2.1)

Value	Description
Name	TR_BSIP_OnlineState
OID	{Root-OID}.2.1
Description	This trap is triggered if a BSIP-ONLY changed its state (Online, Offline)

Value	Description
MAC	MAC address of the associated BSIP
Name	Name of the associated BSIP
Event	Possible events are: **ONLINE, OFFLINE**
Severity	The assigned severity value is "1"

TR_BSIP_SyncState ({Root-OID}.2.2)

Value	Description
Name	TR_BSIP_SyncState
OID	{Root-OID}.2.2
Description	This trap is triggered if a BSIP-ONLY changed its sync state (InSync, OutOfSync)

Value	Description
MAC	MAC address of the associated BSIP
Name	Name of the associated BSIP
Event	Possible events are: **InSync, OutOfSync**
Severity	The assigned severity value is "2"

TR_10_OVL100 ({Root-OID}.2.3)

Value	Description
Name	TR_10_OVL100
OID	{Root-OID}.2.3
Description	This trap is triggered, if the **OVL100** counter has been triggered for **more than 10 times** within the **current day**.

Value	Description
MAC	MAC address of the associated BSIP
Name	Name of the associated BSIP
Event	Possible events are: **OVL100**
Severity	The assigned severity value is "2"

5.4.1.2 DHCP

Due to the specific architecture of the HPCIP system, some special conditions have to be considered for the design of the DHCP functionality.

- In contrast to common VoIP phones (which are equipped with a local console - keypad and display), the BSIP has no local Console access. In case of IP configuration errors (e.g. due to a incorrectly configured DHCP server), if the WBM of the BSIP-IWU is not accessible anymore there is no possibility to correct the error by changing the IP configuration locally.

- In contrast to common VoIP phones (which only have one registration at the PBX), the HPCIP registers several users at the PBX. Errors in the IP configuration of the IWU impact ALL user registration of the IWU.

Taking all the circumstances into account, the implementation of the DHCP client at the IWU was realized in the following way:

- The Default state of DHCP is disabled.

- The DHCP client at the HPCIP-IWU cyclically send a DHCP Request.

- DHCP may only be activated for the Infrastructure network. The IP configuration of the DECT network has to be done manually with a fixed IP address.

- If the DHCP client received a valid DHCP lease from a DHCP server, these values will overwrite the manual IP configuration of the infrastructure network.

5.4.1.2.1 Implementation Detail for Deactivated DHCP

If DHCP configuration was deactivated when the system booted, the following rules apply.

- The manual configured IP configuration will be used

- After activating the button [Network State], a DHCP request will be initiated. The result of the request will be displayed (after a specific timeout) in the output window, independently of the DHCP state (enabled or disabled)

- If the DHCP request has been answered by a DHCP server (DHCP LEASE) the assigned values are displayed, otherwise a timeout message will appear.

- Possible resulting differences between the last IP configuration values and the new values are marked specially.

- For the IP changes to come in effect, a reboot of the IWU is required

- After initiating a reboot process by clicking the [Reboot] button, a new DHCP request will be issued. If new values have been assigned meanwhile, these values are displayed. This ensures, that that the current assigned values are printed out at the WBM.

- If the DHCP flag has been toggled to enabled, and a DHCP REQUEST was successful, the newly assigned IP address values are stored inside the configuration.

- Activating the DHCP flag disables the editing of the manual values

- **Important Note:** All DHCP settings (as well as the manual IP settings) apply to the active system partition.

5.4.1.2.2 Implementation Detail for Activated DHCP

If DHCP configuration was activated when the system booted, the following rules apply.

During the start up phase of BSIP-IWU

- The DHCP client automatically starts and emits a DHCP REQUEST

- If the DHCP client receives a positive acknowledge within a specific period of time (response time), the assigned IP configuration will be applied to the IWU.

- If no DHCP server responds within the response time then, the last stored IP configuration will be applied to the IWU

- The output of the [Network state] button displays the results of the last DHCP REQUEST

During the operation mode of BSIP-IWU

• Refer to the procedures described before (after applying button network state)

5.4.1.3 Ethernet Synchronization (acc. IEEE1588)

Towards an Ethernet based Synchronization (acc. IEEE1588, PTP Precious Time Protocol) great demands are made on Ethernet characteristics like symmetry, packet loss, delay, jitter (variation of delay). Therefore special requirements regarding the Ethernet components (especially the Ethernet switches used) have to be considered. Exceeding of limits (especially of jitter) will lead to loss of synchronization, which will finally lead to a resynchronization process. During this process the belonging Base Stations are unable to establish telephony connections.

The Synchronization according Ethernet solely uses a star shaped topology. Maximally one Base Station (BSIP-Only) serves a Synchronization Master (Sync Master), all other Base Station which participate at the synchronization serve as Synchronization Slaves (Sync Slave).

Resynchronization

The DECT functionality of all BSIP, which are configured as IEEE1588 Sync Slaves, depends on the availability of the IEEE1588 Sync Master. If the Sync Master is not functional (e. g not Online due to Ethernet problems …), all 1588 sync slaves will go OutOfSync. During this time no telephony is possible.

General requirements on the Ethernet system

A maximum number of three cascaded Ethernet switches are supported between the Sync Master (SM) and a Sync Slave (SS) BSIP. The following figure illustrates a valid and an invalid setup according the "3 switch hop" rule.
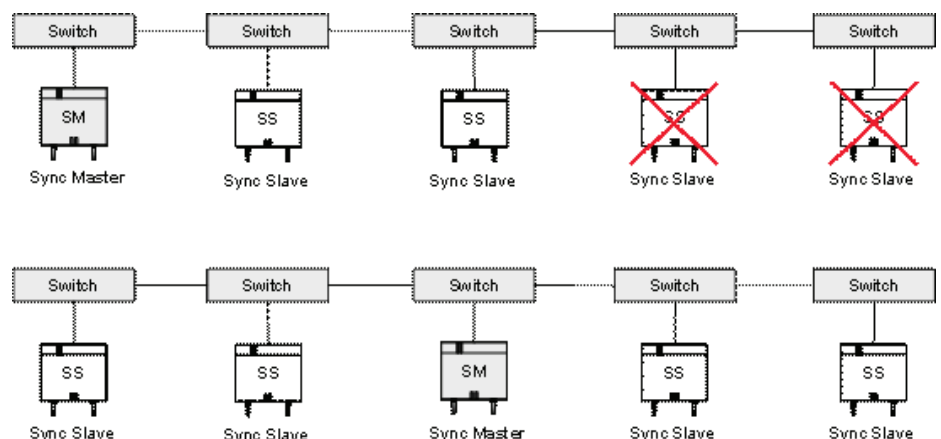
As shown in this figure, also a 5 switch setup may be realized by choosing the correct position of the Sync-Master inside the switch topology.

Only premium class switches, which fulfill the requirements regarding Ethernet synchronization according IEEE1588, are supported. A list of supported switches is documented in the HPCIP Wiki pages at http://wiki.siemens-enterprise.com/index.php/HiPath_Cordless_IP_-_IEEE_1588.

Usage of VLAN at the BSIP-IWU for Infrastructure and DECT network is mandatory. All participating switches have to be configured in a way that the VLAN of the DECT network has to be assigned the highest priority.

5.4.1.4 VLAN Configuration Example

The following figure depicts a sample setup of a system which uses Ethernet Synchronization acc. IEEE1588 in combination with VLAN, CoS and multiple switches.
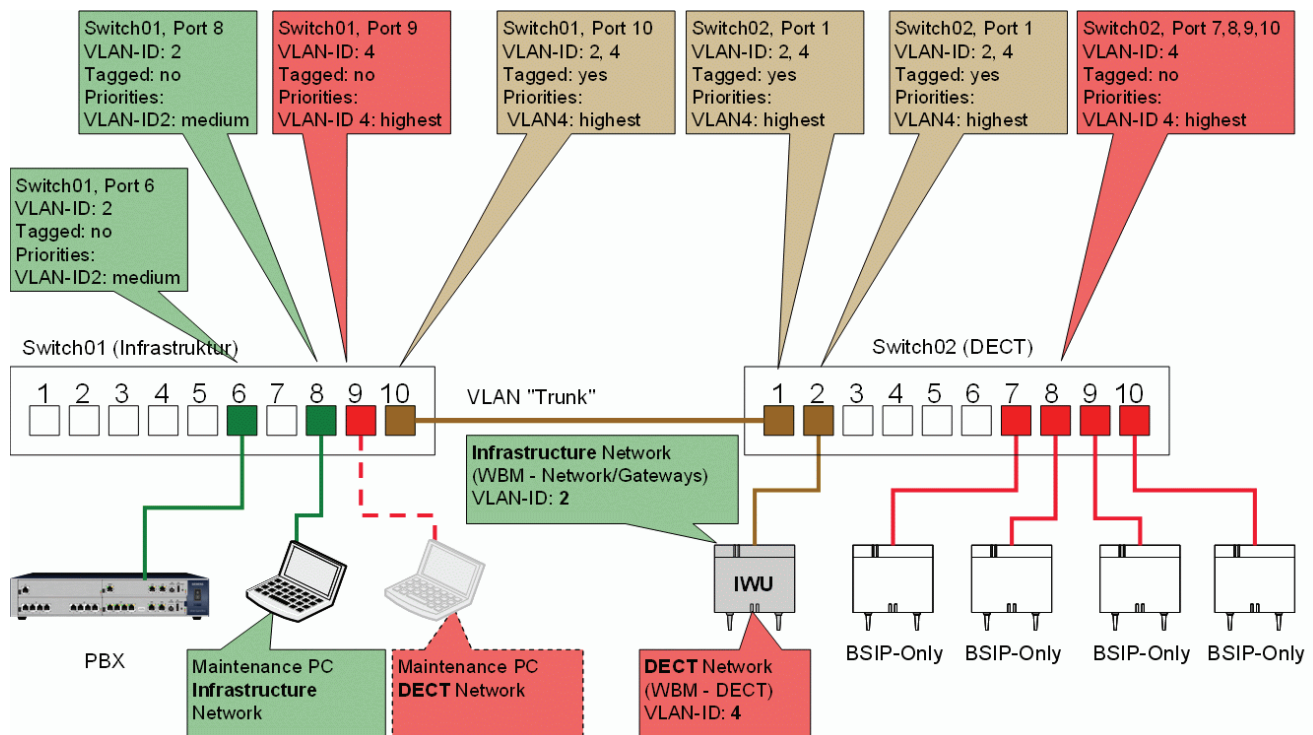
5.4.1.5 Codec G.729

5.4.1.5.1 General G.729 hints

The codec implementation which is used for the HPCIP system uses G.729ab mode (including silence suppression).

Please keep in mind that G.729.ab requires less bandwidth between the IWU and the PBX. As a drawback, the voice quality of G.729ab connection is not as good as compared to G.711 connections. Using G.729ab for voice connections requires more system resources at the IWU. Therefore, the maximum number of parallel connections for the IWU of HPCIP (BSIP-IWU) will lower the maximum number of calls from 10 to a specific value (depending on the number of G729 and parallel G711 calls). For details refer to chapter 5.4.1.5.2, "Call Control for G.729 Call Limiting (BSIP-IWU only)".

In contrast to the BSIP-IWU (which has very limited CPU performance compared with the Server-IWU), on a Server-IWU all 50 calls may be established using G.729.

The codec may be activated on a per-user base (See column "G729" at page User - Voip), even during running system services using the [Edit User] button.

The usage of G.729 codec is mainly intended for low bandwidth connections (WAN). In contrast, G.711 connections are mainly preferred inside the LAN where bandwidth should not be an issue.

Depending on the gateway used, internals calls between two enabled G729 users are also established with G.729. To overcome this situation the PBX has to control the codec negotiation between different users. The only capable gateway with codec negotiation between SIP subscribers is OpenScapeVoice using the "CAC Codec Manipulation" feature.

Activating codec G.729 extends the codec list (which is used for the SIP SDP), provided that the Call Control feature doesn't alter the codec list.
The codec list excluding G.729 is (in descending priority order): "G.711a, G.711u".
The codec list including G.729 is (in descending priority order): "G.729ab, G.711a, G.711u".

Depending on call direction and remote station (especially the G.729 priority) calls are negotiated with the following codecs:

Table - codec negotiation

Call initiator —— Call receiver		HPCIP		SIP phone (optiPoint, OpenStage)		
		G.711	G.729 G.711	G.711 G.729	G.729 G.711	G.729 exclusive
HPCIP	G.711	G.711	G.711	G.711	G.711	No call estab-lishment 2)
	G.729 G.711	G.711	G.729	G.729	G.729	G.729

Call initiator / Call receiver		HPCIP		SIP phone (optiPoint, OpenStage)		
		G.711	G.729 G.711	G.711 G.729	G.729 G.711	G.729 exclusive
SIP phone (optiPoint OpenStage)	G.711 G.729	G.711	G.711			
	G.729 G.711	G.711	G.729			
	G.729 exclusive	Hangup after Connect 1)	G.729			

1) Call Processing receiver is alerting After Connect of B-party call Disconnects.
2) Call Processing receiver is NOT Alerting due to common codec.

Interoperability with optiPoint 150 S

If using the OP150S with activated G.729, the option "Silence suppression" has to be disabled. Otherwise, the G.729 voice connection between an OP150S and a HPCIP handset will de disturbed.

5.4.1.5.2 Call Control for G.729 Call Limiting (BSIP-IWU only)

A call control feature has been added limit the number of G.729/G.711 connections at a BSIP-IWU. The limits are adapted dynamically (depending on the number of G.729 and G.711 calls). G.729 requires more CPU resources than G.711 connections.

The Call Control limits the following values:

• Number of calls depending on the actual combination of G.729 and G.711 calls (see codec table below) and

• Limits the codec list to G.711 only, if these values are reached, so further calls are restricted to G.711.

Two call conditions have to be differentiated (see table below):

1. The Maximum Call Limit is reached. No further calls may be established or accepted.

2. A Partial Call Limit is reached. Further calls may only be established or accepted with codec G.711.

Handling of Maximum Call Limit

- For an outgoing call (Handset -> PBX) at the handset "Channel occupied" is displayed and a Busy tone is played.

- For an incoming call (PBX -> Handset), the call is refused at the SIP-Interface with a SIP message "503 Service unavailable".

Handling of Partial Call Limit

- For an outgoing call (Handset -> PBX), codec G.729 is removed from the codec list at the SIP-Interface in the INVITE message. Therefore the codec list will only include G.711 codecs G.711a and G.711u.

- For an incoming call (PBX -> Handset), codec G.729 is removed from the codec list at the SIP-Interface in the OK message after the Call was accepted at the handset. Therefore the codec list will only include G.711 codecs G.711a and G.711u.

- Depending on the PBX used and the configuration of the remote party (especially for devices which use G.729 exclusively), the call may be not signaled at all or disconnected after the hook-off procedure.

Table of Call Control Limits

Partial Call Limit		Maximum Call Limit
Max. no. of G.729 calls	Max. no. of G.711 calls	Max. no. of calls
6	0	6
5	2	7
4	3	7
3	6	9
2	8	10
1	9	10
0	10	10

- **Hint:** The values inside this table are valid for a BSIP-IWU which sync configuration is "No sync", "AIR Slave" or "AIR Master".

Examples for call Control Limits

5 x G.729 calls and 1 x G.711 call are already active. A further call is limited to G.711, since a possible combination of 6 x G.729 and more than 0 x G.711 calls is not supported (see table).

5 x G.729 calls and 2 x G.711 calls are already active. A further call is rejected, since the Maximum call limit (7) for this codec combination is reached.

4 x G.729 calls and 2 x G.711 calls are already active. A further call may be established using G.729, since a combination of 5 x G.729 and 2 x G.711 calls is supported (see table).

3 x G.729 calls and 5 x G.711 calls are already active. A further call is limited to G.711, since a combination of 4 x G.729 and more than 3 x G.711 calls is not supported (see table).

2 x G.729 calls and 7 x G.711 calls are already active. A further call is limited to G.711, since a combination of 3 x G.729 and more than 6 x G.711 calls is not supported (see table).

- **Hint:** Running a BSIP-IWU with a high number of BSIP-Only (>5) and a high number of configured users (>30) configured users while having a maximum amount of call established will slow down the WBM interaction. For planned service issues (e.g. re-configuration, adding users or BSIP) it is recommended to schedule these actions in a time frame of low call utilization, since this will improve WBM; interaction.

5.4.1.6 Timezone Support

A Timezone may be selected on WBM page Network/Gateways. This timzone defines the time shift to GMT (Greenwich Mean Time) as well as the parameters for daylight savings. About 75 different time zones are available, which should cover nearly all regions of the world.

The appropriate Timezone for Germany is:

"(GMT +01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna".

- **Hints:**
  Activating a changed timezone setting requires a reboot of the IWU. Configuration of a Timezone on a BSIP-IWU is reasonable only in the context of a configured NTP server.
  The width of the timezone column may be changed by dragging the scale element at the lower right corner (see figure).
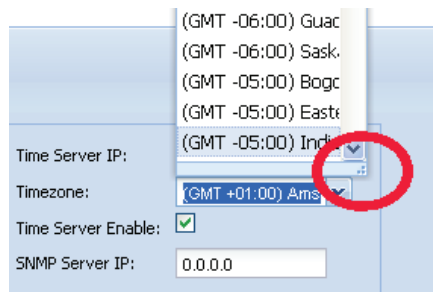
5.4.1.7 SIP Survivability

5.4.1.7.1 Support of Outbound Proxy

Choosing the outbound proxy option in the HiPath Cordless IP solution means, that all SIP related traffic is routed directly to the outbound proxy, independent from the domain name or IP address that is configured for the SIP server/proxy/registrar.

For each SIP gateway of the HPCIP solution the option "Outbound Proxy" can be activated / deactivated per checkbox.

In case outbound proxy is activated, a valid IP address must be entered in the field "Outbound Proxy" (For this option, the usage of a domain name is not possible).

If the outbound proxy checkbox is unchecked, the IP address in the "Outbound Proxy" field is ignored. In that case the IP address for signaling will be derived from the input in the "SIP server Id" field. If this input is a domain name (FQDN), DNS is used to resolve the domain name. If more than one IP addresses are returned, only the first will be used and the other will be ignored. The DNS request will be repeated each hour (to recognize configuration changes in the network).

If the IP address of the "SIP Server Id" changes after a DNS request, the new IP address will be used for the next Re-Register or if a call setup has failed with a timeout. The Re-Register timer is here 120 seconds.

5.4.1.7.2 DNS Administration

DNS servers may be configured system wide ("System DNS") or gateway specific.

After activating the gateway specific feature "DNS SRV" the IP addresses for the primary and secondary DNS server (valid for all "SIP gateways") can be entered. In case, DNS server IP addresses are received via DHCP, they will entered in the system DNS fields.

In addition for each "SIP gateway" two DNS IP addresses can be entered. They will be used when the System DNS option checkbox is empty.

5.4.1.7.3 DNS SRV

To use DNS SRV, outbound proxy mode must be deactivated.

DNS SRV will be activated with a checkbox for each "SIP gateway". In that case the input fields for outbound proxy will be ignored. The DNS administration for resolving domain names is the same as described above.

If DNS SRV is activated, the HPCIP uses the fully qualified domain name in the "SIP Server Id" field to send a DNS SRV request for a service (SIP) and the protocol name (UDP).

The answer contains a prioritized list of hosts (FQDN) providing the service. If the hosts are not already resolved to an IP address in the same DNS SRV response, HPCIP needs to perform an "A record lookup" for these hosts.

The DNS SRV request will be repeated each hour. If the DNS response contains a Time-to-live parameter, this value will be used for the refresh timer.

If the HPCIP system detects a failure in the communication with the SIP server, the next IP address in the SIP server record list is used.

In the WBM the status page (Calls Dect) is updated to show the IP address actually used for REGISTER and INVITES (in case of an active call) and the list of SIP server ID addresses resolved with DNS SRV. IP addresses in the penalty box are marked (see output of [Network state]).

The number of IP addresses, that can be used out of a DNS SRV answer, is limited to 5.

- **Important note:** If using DNS SRV, the whole system functionality mainly depends on the availability of the configured DNS servers. If the DNS servers are not reachable during start of HPCIP system services, the gateways configured with DNS SRV are not functional at all. If the DNS servers are not functional during a DNS poll cycle, the last DNS list received by the DNS servers is used instead.

5.4.1.7.4 Penalty Box

If the communication with a SIP server fails (timeout or server error messages), the IP address of this SIP server gets into the penalty box for 10 minutes and the next prior IP address of the DNS server record list is used for registration and call setup. After 10 Minutes the IP address is back for that specific "SIP gateway". This address will be used for each new Re-Register message and for each new INVITE message for all handsets assigned to this "SIP gateway", active calls are not affected. Therefore active calls are disconnected (at least after a RAS_DOWN event for the user).

- **Hint:** The current state of the penalty box may be derived from the output of [Network State] (see chapter 5.4.1.7.7, "Survivabilty Information").

5.4.1.7.5 SIP NOTIFY Message in Limited Mode

If the connection between a branch proxy and the OSV fails, the branch proxy turns into limited mode with reduced feature set. To inform the clients in the branch a SIP NOTIFY message is sent to the phones. In the case of HPCIP system there will be no indication in the handsets in idle mode about the limited mode. Since it is necessary in DECT to place a call to write something on the idle screen, performance issues forbid an idle mode display text. In addition the display of a portable handset is not watched regularly, so an idle display text is not really useful. Therefore "Limited Mode" is shown on the display in case of Call setup for incoming or outgoing calls. In case of an active call during reception of the SIP NOTIFY message, no action for that handset take place at all.

If OpenScape Branch OSB goes into survivability mode the OSB sends a Notify message for each phone to the HPCIP server (Event: server-mode-backup). The HPCIP server sends 200OK back for each NOTIFY message.

When OSB goes back to normal mode another NOTIFY (Event: server-mode-normal) is sent from the OSB for each subscriber and a 200 OK is received for each NOTIFY.

5.4.1.7.6 Detection of Failure of SIP Servers

Since HiPath Cordless IP support SIP over UDP only, a failure of the connection to a SIP server is only detected by SIP signaling timeouts (The reception of a SIP 503 response code will not be interpreted as a server failure.). Therefore the detection of a SIP server outage will be detected at latest with the next re-register cycle (default: 120 sec.).

*   **Hint:** OSV is able to send a "retry-after" value in the REGISTER response message (OpenScape Office and H4K will not do so). Therefore the Re-Register interval may be controlled by the OSV.

5.4.1.7.7 Survivabilty Information

The output of [Network State] on page Administration contains important information about SIP Survivabilty.

Example output:

```
### Network configurations of HPCIP - Server ###
## ApplicMode Iwu ##
## Network / Gateway settings ##
Ip Address            : 192.168.100.112
Network Mask          : 255.255.255.0
Default Gateway       : 192.168.100.101
DHCP enabled          : FALSE
Dns Server 1          : 192.168.100.226
Dns Server 2          : 192.168.100.227
...
## Gateway ##
001: <                 OSOMX3bx> Ip 1 : <192.168.100.230>:5060
002: <                 OSOMX1bx> Ip 1 : <192.168.100.226>:5060
003: <                   OSV50> Ip 1 : <192.168.100.204>:5060
004: <          DNS-SRV-GW> Ip 1 : <192.168.100.111>:5060 PenaltyBox <yes>
004: <           DNS-SRV-GW> Ip 2 : <192.168.100.112>:5060 PenaltyBox <no>
004: <           DNS-SRV-GW> Ip 3 : <192.168.100.113>:5060 PenaltyBox <no>
```

5.4.2 Configuration Techniques

5.4.2.1 Free IP Addressing

Starting with V1R2 the possibility of free IP addressing and therefore full functionality of the Default Gateway support is supported.

Free ip addressing

In V1R1 the DECT network was statically configured to 192.168.0.0/16 (192.168.0.0 255.255.0.0). Starting with V1R2 the DECT network is now freely configurable by means of configuring DECT ip address and the corresponding netmask.

The following restrictions apply:

• Infrastructure network and the DECT network have to be different (they also may not overlap).

• If adding factory equipped Base stations (running V1R1) to a V1R2 or V1R3 HPCIP-IWU, they will not be scannable if the Dect network is different from 192.168.0.0/16.

For details regarding these issues refer to chapter 5.4.2.2.1, "Scanning of BSIP (V1R1) with IWU (V1R2 or V1R3)".

Default gateway support

In V1R1 the DECT network was statically configured to 192.168.0.0/16 (192.168.0.0 255.255.0.0).

If some components of the infrastructure (PBX, NTP Server, Configuration PC, ...)

• were located inside a network of 192.168.x.y and

• were located behind the default gateway,

the default route - using a configured "Default Gateway" - was without function (since the IP stack of HPCIP-IWU treated all 192.168.x.y addresses as local due to the DECT network configuration).

As a workaround, one single static route could be configured (see "Network desti-nation" / "Network mask" / "Gateway" at page Network/Gateways).

5.4.2.2 Adding new BSIP

If version V1R2 or V1R3 is running, it is possible to configure a netmask for the DECT IP network. In V1R1 the network address as well as the netmask was fixed (192.168.0.0 with a netmask of 255.255.0.0).

Now it is possible to configure the DECT IP network freely and assign it a netmask.

Due to routing issues, this netmask may be changed to 255.255.255.0 when also using a CLASS C ip network (192.168.x.y) for the Infrastructure network.

5.4.2.2.1 Scanning of BSIP (V1R1) with IWU (V1R2 or V1R3)

As a drawback, when adding factory equipped Base stations (running V1R1) to a HPCIP-IWU (running V1R2), they will not be scannable (since they didn't respond to SCAN requests others than 192.168.255.255).

• **Important note:** The following instructions apply to newly added BSIP which have version V1R1 running. If they are already running V1R2 or V1R3 there are no special steps to consider.

There are two different procedures to overcome of this situation:

1. **Manually update the newly added BSIP locally**

   This method is suitable if a small amount (one to three) BSIP should be added.

   Manually connect the first new BSIP and connect to its local WBM. Initiate a local update to the same version as running on the IWU. If the active partitions differ between IWU and BSIP after updating and rebooting, login again and initiate the update again to synchronize the partitions between IWU and the newly added BSIP.

   Disconnect the currently updated BSIP from the network and attach the next one (otherwise there will be IP address conflicts since all factory reset BSIP are equipped with 192.168.1.1) and then follow the instructions below.

2. **Temporarily move the DECT network to V1R1 settings**

   This method is suitable if a great amount (more than three) BSIP should be added.

   Temporarily revert to a DECT IP address inside the range of 192.168.0.0 and assign a network mask of 255.255.0.0 but remember that the temporarily DECT network can't overlap with the Infrastructure network, Apply the changes, SYNC the Base stations and reboot the system. If applicable, do a further update into Partition 2 (since all factory delivered BSIP are active in System partition 2).

   After a SCAN the newly added BSIP are displayed on page Dect. Configure the necessary settings SYNC the newly added base stations and reboot into the updated partition.. If all BSIP are in the desired state ONLINE=YES (see page Status) initiate a firmware update with V1R3. After reboot revert to the former DECT network parameters, SYNC and reboot the system.

5.4.2.3 Multi-Register (Bulk Registering) of Handsets

The multi register feature eases the configuration process if registering a large amount of users remarkably. Adding a large amount of users in V1R1 required a lot of manual configuration and intervention of the administrator. Firstly, all users have to be added and configured inside the WBM. Afterwards, while registering the handsets the correct user entry has to be located and marked and then regis-

tering both at the WBM and at the handset has to be initiated. The new bulk registration process now simplifies these processes by auto-adding a new user entry and then simply assign the next DECT handset registration to the last user.

To start the multi register process, at least one user entry (with start values) has to be configured manually. This user entry serves as the template user for the users which will be added.

Select an existing, enabled user entry.

After clicking on [Multi register] a handset may be registered directly. After successful registering of the handset, a new user entry will be added which is populated with the IPUI of the registered handset. For this entry, values are incremented by default. Now the next handset may be registered. This process may be repeated several times.

The Multi Register process may be stopped by using the [CANCEL] button.

• **Hint:** This feature is available in Siemens Admin mode only.

The following table gives an overview how the new values are created. The user template is the user which was selected initially before starting the Multi Register process.

Option	Action for new value
Index/DisplayIndex	Will be **incremented** automatically
Enabled	**Copied** from option "Enabled" of the user template
Msn	**Incremented** from option "MSN" of the user template
DisplayName	**Incremented** from option "MSN" of the user template
Comment	**Incremented** from option "MSN" of the user template
Language	**Copied** from option "Language" of the user template
Groups	**Copied** from option "Groups" of the user template
UserName	**Incremented** from option "UserName" of the user template
AuthName	**Incremented** from option "AuthName" of the user template
Password	**Copied** from option "Password" of the user template
G729	**Copied** from option "G729" of the user template

• **Further Hints:**

  • If the TemplateUser is not assigned a handset already (IPUI = "00000000") the first DECT Registration of the MultiRegister will be applied to this User.

  • If the TemplateUser is assigned a handset already (IPUI ? "00000000") the first DECT Registration of the MultiRegister will be applied to the first new user. This ensures that an already existing registration at the TemplateUser will not be overwritten.

- If one of the intended auto incremented numbers already exist in the configuration, it is omitted automatically.

- After creation of an added user it is registered automatically at the PBX.

- The multi register process is not stopped by a timeout. It has to be finished using the [CANCEL] button.

5.4.2.4 Downgrading a HPCIP System

After a BSIP factory reset has been initiated, the factory defaults are restored. If a complete HPCIP system (IWU and Base Station) has been downgraded, the following items have to be considered.

After a factory downgrade of a BSIP-IWU system, take attention to which MAC address you are connecting to change the working mode of the BSIP (BSIP-Only to BSIPIWU). If you simply connect to 192.168.1.1 you may be connected to ONE of all attached BSIPs. This may not be the designated BSIP (former BSIP-IWU).

Therefore disconnect all other BSIP from the Ethernet or attach the designated BSIPIWU to a direct Ethernet connection at the Maintenance PC. Login to this BSIP via WBM and change the application mode to IWU mode. Afterwards you may connect the other BSIP-Only to the Ethernet.

- **Hint:** The MAC address is shown at page Administration - Program Info - Version System.

5.5 Configuration Hints for PBXs

In the following chapters you can find configuration notes for for different PBXs which have to be released for usage with the HiPath Cordless IP system.

5.5.1 OpenScape Office MX (OSO MX)

Here you can find the configuration hints using a Siemens OpenScape Office MX (SW-Version V1) using SIP users.

5.5.1.1 Base Configuration - OSO MX

The following value is used for the base configuration:

Parameter	Value
IP address of the OSO MX	192.168.0.93

Detailed configuration instruction for the OSO MX would go beyond the scope of this documentation. Therefore only the information regarding the configuration which is very important and relevant for the interworking is described here.

Detailed documentation for the OSO MX may be found in the manual:

• "OpenScape Office MX V2, Administrator Documentation"

1. Please configure the OSO MX for the usage with SIP Users and configure the needed number of SIP Users in the Installation Assistant.

2. Configure the IP address of the OSO MX to 192.168.0.93 or change the according IP addresses.

3. Configure the following Codec Parameters via "WBM - Expert mode - Voice Gateway - Codec Parameters":

4. Configure the DSP Settings (primarily the Echo Cancellation) via "WBM - Expert mode - Payload - - HW Modules - Edit DSP Settings":

5.5.1.2 Base Configuration - BSIP-IWU

Please perform the following configuration settings at the BSIP-IWU:

Page "Gateways"

Entry	Value
SIP Server Id	192.168.0.93

1. Save all modifications with [Apply].

2. Configure one BSIP for the operation with this Gateway.

5.5.1.3 Station Configuration - OSO MX

The following values are used as a sample for this configuration instruction:

Parameter	Value
Name	DECT-761
Callnumber	761
Password	1234

The configuration of the OSO MX is done via Web browser (Web Based Management - WBM).

1. Please log in to the OSO MX, start the Web Based Management in Expert mode and navigate to the page "WBM - Expert mode - Station - IP Clients - SIP Clients".

2. Select a free entry (after the base configuration of the OSO MX with the Assistant free entries should be available).

3. If no free entries are available, use the page "WBM - Expert mode - Stations - Station - IP Clients - Edit subscriber", change the "Device Type" of a free entry to "SIP Client" and store the modifications with [Apply]. Now a free SIP User should be available on "WBM - Explorers - Stations - Station - IP Clients - SIP Clients".

5.5.1.3.1 Step 1 - User Parameters

Select the free entry and choose "Edit station parameter".
Enter the following values in the input mask:

Entry	Value
Callnumber:	761
Name:	DECT-761

Entry	Value
Direct inward dialing:	761

Please do not change the other values. After that the configuration page should look like this:

5.5.1.3.2 Step 2 - Workpointclient Data

Select the free entry and choose "Edit Workpointclient data".
Enter the following values in the input mask:

Entry	Value
Authentication active:	[V]
Password:	1234
Validate password:	1234
User ID:	761
Realm:	761

Please do not change the other values.

After that you should save the new configuration on the HiPath with the [**Apply**] Button at the bottom of the WBM.

5.5.1.4 Station Configuration - HPCIP IWU

Please make the following configurations at the BSIP-IWU:

Page "Users - User"

1. Go to the sub page "User" of "Users" in the Configuration Utility.

2. Select the first entry "DisplayName" and enter the following values:

Entry	Value
DisplayName:	761

3. Save the modifications by clicking [**Apply**].

Page "User - VoIP"

1. Select the first entry and enter the following values:

Entry	Value
MSN	761
UserName:	761
AuthName:	761
Password:	1234

2. Save the modifications by clicking [**Apply**].

5.5.1.5 Time server configuration

1. Configure the following settings to activate the time server settings via "WBM - Expert mode - Basic Settings - Date and Time - SNTP settings":

Entry	Value
Administration mode of SNTP client:	Up
IP address / DNS name of External Time Server	IP adress: 0.0.0.0 if no external time server is used for time synchronisation, otherwise the IP address of the external time server.
Poll interval for External Time Server	Continuous

2. Save the modifications by clicking [**Apply**].

5.5.2 HiPath 3000

This chapter contains configuration hints to configure a Siemens HiPath 3000 for usage with a HPCIP system using SIP subscribers.

5.5.2.1 Base Configuration - HiPath 3000

1. Please configure the HiPath 3000 for the usage with SIP Users and configure the needed number of SIP Users in the Installation Assistant.

2. Configure the following Codec Parameters via "WBM - Expert mode - Explorer - Voice Gateway - Edit Codec Parameters". Frame Sizes of 20 msec are required (mandatory)!

3. Configure the DSP Settings (primarily the Echo Cancellation) via "WBM - Expert mode - Explorer - Payload - HW Modules - Edit DSP Settings":

5.5.3 HiPath 4000

This chapter contains configuration hints to configure a Siemens HiPath 4000 for usage with a HPCIP system using SIP subscribers.

5.5.3.1 Base Configuration - HiPath 4000

1. Please configure the HiPath 4000 Softgate or the HG3500 unit for the usage with SIP Users and configure the needed number of SIP Users in the Installation Assistant.

2. Configure the following Codec Parameters via "WBM - Expert mode - Explorer - Voice Gateway - Edit Codec Parameters". Frame Sizes of 20 msec are required (mandatory)!

3. A configuration of the DSP Settings (primarily the Echo Cancellation) is not possible, since no DSP is available.

4. The SIP users have to be assigned the parameter MBCHL (Multi BCHANNEL) in AMO-SDAT.

5.5.4 OpenScape Voice (OSV) V4R1

This chapter contains configuration hints to configure a Siemens OpenScape Voice for usage with a HPCIP system using SIP subscribers.

5.5.4.1 General - OSV

There are 2 different setups for usage of HPCIP connected to OpenScape Voice (OSV).

HPCIP is connected to OpenScape Voice directly:

HPCIP is able to communicate with one OpenScapeVoice-SIP-address only. In case of geographically separated OSV-cluster the nodes have different Signaling-IP-addresses in different IP-subnets. Therefore HPCIP Users can only be connected to OSV-Node1 or to OSV-Node2. If this node will fail no communication via HPCIP would be possible anymore.

This problem does not exist if HPCIP is connected to a co-located OSV-cluster until 2nd OSV will take over the Signaling-address of the 1st node in case of node-failure.

If the HPCIP system has to be connected to a geo-separated OSV it is recommended to include OpenBranch, which is described below.

HPCIP is connected to OpenScape Voice via OpenBranch:

In this setup scenario HPCIP is communicating with OpenBranch-SIP-address only and OpenBranch-proxy is forwarding all SIP-messages to OpenScape Voice. To avoid a single-point-of-failure at OpenBranch-side it is strongly recommended to set up OpenBranch redundantly (using VRRP).

In case of node-failure in a clustered-OSV OpenBranch will address HPCIP-messages to the remaining OSV-node (doesn't matter if co-located or geo-separated OSV is used).

5.5.4.2 Base Configuration - OSV

HPCIP endpoints have to be configured in the same way in OSV-configuration as other SIP-users do. OSV does not know anything about the HPCIP DECT system. All HPCIP users will register at OSV with the same IWU address.

Workaround for Call-Forwarding:

There is one necessary workaround to configure HPCIP users as keysets. Otherwise call-forwarding to DECT-IP-users will not work. No secondary-lines have to be configured here.

Keyset-Operation has to be set to Primary in OSV subscriber-administration. This is a valid workaround for currently released OSV-versions (V4R1, up to patchset 29-Exx) only. This may be changed in later versions of OSV.

Usage with OpenScape Web client:

If HPCIP users are used with OpenScape web client the HPCIP users feature-profile should be set to CSTA = Normal.

Only Limited feature-set using web client is supported.
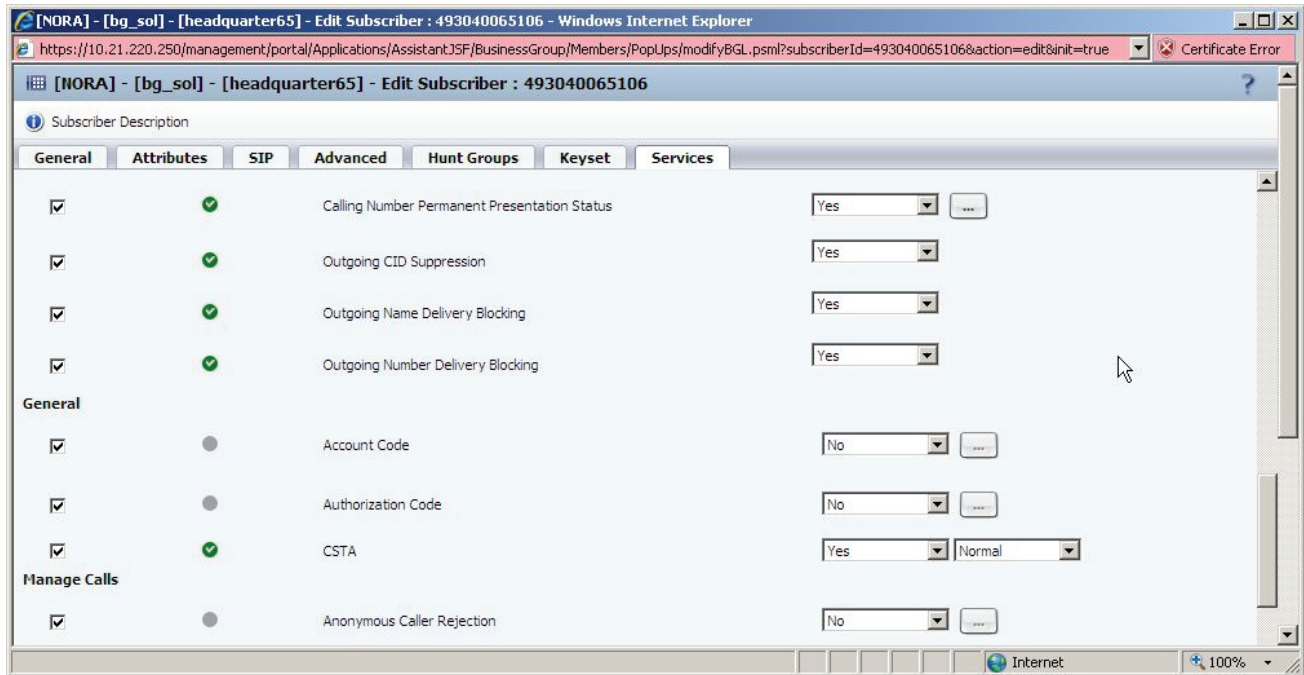
Configuration of Gateways (Page network / Gateways)

Each SIP-server (OpenBranch and/or OpenScapeVoice-signaling-IP-addresses has to be specified here).

Different HPCIP users from one system may register on both Geo-separated OSV-nodes or on OpenBranch. In standard customer-scenarios only one gateway will be used.

For Geo-separated OpenScape Voice:

If the HPCIP IWU is directly connected to a Geographically-node-separated OSV-cluster (Main-Office, no OpenBranch-Proxy involved) it is necessary to enable Flag "Direct Signaling". Otherwise calls from phones located on the 2nd node will not be accepted by HPCIP. If this flag is disabled the IWU allows only calls from the IP-address where the HPCIP user is registered to. If this flag is enabled HPCIP allows calls from any IP-addresses.

So for security-reasons this flag should only be enabled if HPCIP is used in Geo-separated OSV.

Page User - Voip

The "Msn" should be identical to "UserName", both are in E.164-format.

The options "AuthName" and "Password" are necessary if Digest-Authentication is enabled in OpenScape Voice.

5.5.4.3 Limitations

- One HPCIP user can communicate with one SIP-server-address only. A failover of a 2nd SIP-server-IP-address is not supported yet.

- Limited UC-functionality if OpenScape web client is used

- Only SIP transport-protocol UDP is supported for HPCIP-users

- Limited feature Pickup-Group for HPCIP-User (no audible/visible Call-Indication at Handset)

- Feature Call-waiting is not available

- Only packet-size 20 msec with codec G.711 is currently accepted by HPCIP. gateways have to be configured to also use 20 msec toward the HPCIP IWU.

- Call-forwarding to IP-DECT-users is currently only possible if HPCIP-user is configured as Keyset in OSV-configuration

5.6 Troubleshooting / FAQ

5.6.1 DECT

5.6.1.1 BSIP-Only is not found using "Scan"

Please check the following:

• Is the "missing" BSIP connected with the power supply?
  (LED states OK?)

• Is the network cable connected at the IP-DECT Base Station?

• Is the network cable connected to an Ethernet Switch? Please check the
  Status LEDs at the relevant Ports of the Ethernet Switch.

• The IP-DECT Base Station must be located in the same Ethernet segment as
  the IWU. IWU and Base Station cannot operate in different Ethernet
  segments connected via an IP Router.

• VLAN configuration issues

• Newly added BSIP are not recognized and displayed by SCAN during running
  system services. Stop the system services and repeat the SCAN.

• If firmware V1R1 is already running on BSIP, some further restrictions may
  apply. For details refer to chapter 5.4.2.2.1, "Scanning of BSIP (V1R1) with
  IWU (V1R2 or V1R3)".

5.6.1.2 Registration of the handset is not successful

• The PIN configured for the IWU differs from the PIN entered at the Handset
  (Did you mistype?).

• The handset has no radio connection to the Base Station (too far away etc.).

• Are all activated Base Station in state "Online" and "InSync" (except the Base
  Station which is the Synchronization masters) ?

5.6.1.3 Idle display of handset is blinking

The following causes may apply:

• the handset is outside the DECT coverage

• the handset has no DECT registration at the BSIP

- at the handset the wrong base is selected or

- the system services are not running

5.6.1.4 Display message "Netzfehler" / "Out of Order"

The RAS registration from the handset at the PBX is down (see Status - Calls Dect - Voip states)

5.7 Appendix

5.7.1 Configuration hints for Web Browser

5.7.1.1 Mozilla Firefox

Mozilla Firefox Versions 2.x, 3.0.x, 3.5.x and 3.6 are supported.

The minimum supported screen resolution the Browser is running on is 1024x768.

5.7.1.2 Microsoft Internet Explorer

The following version of Microsoft Internet Explorer are supported:

• Version 6.x

• Version 7.x

• Version 8.x

The minimum supported screen resolution the Browser is running on is 1024x768.

Depending of the security settings of MS IE, the IP address of the BSIP has to be added to the list of Trusted sites (Tools - Internet options - Security - Trusted sites).

This comes in effect when Backing up a configuration file. If the security settings are not valid, the configuration file will not be donloaded and the WBM session will be closed.

For **IE7** there is an issue one some installations when backing up the configuration of the IWU. After initiating the backup process, the information panel will be displayed and afterwards you are logged out from the WBM. To overcome this situation, you have to change the following settings in IE7:

1. Select Tools - InternetOptions - Security

2. Select the appropriate zone in which the IWU is located (e.g. "Trusted sites") and select [**Custom level**]

3. In the outline view browse to "Downloads" and change the setting of "**Automatic prompting for file downloads**" from Disabled to **Enabled**.

6 Technical Data

6.1 BSIP1 DECT standard EU

- Number of channels   120 duplex channels, freely administered
  (10 carriers, each with 12 time-division multiplex channels)

- Frequency range   1.88 to 1.9 GHz
  (send and receive range)

- Channel spacing   1.728 MHz

- Bit rate   1.152 Mbps

- Speech encoding   32 kilobit ADPCM

- GAP standard   Specified in DECT specification 300444

- PN CAP   Siemens-specific protocol enhancement

- DECT Access   EN 301 406 V.1.5.1

DECLARATION OF CONFORMITY

We

Siemens Enterprise Communications GmbH & Co. KG

Hofmannstr. 51, D-80200 Munich / Germany

declare that the product

HiPath Cordless Basestation IP1 (BSIP1)

....
(name, type, model or version)

to which this declaration relates, conforms to the following European Directives and European standards:

Directive 99/5/EEC: Radio and Telecommunication Terminal Equipment

EN 50385:2002	EMF
EN 60950-1:2006	Safety
EN 55022:2006+A1:2007 ClassB	EMC, Emission ITE Residential Environment
EN 61000-6-2:2005	EMC, Immunity in industrial area
EN 301 406 V1.5.1	DECT Access
EN 301 489-1 V1.8.1	EMC & Radio spectrum Matters for radio Equipment
EN 301 489-6 V1.3.1	EMC & Radio spectrum Matters for radio Equipment (DECT Equipment)

Other standards or national regulations:

FCC CFR 47, P.15 Class B	Radio frequency devices, radiated Emmission

Munich, March 12th, 2010

Siemens Enterprise Communications GmbH & Co. KG   ....
(Place and date of issue)

Stephan Schaade

(Name, Function and signature of authorized person)   (Name, Function and signature of authorized person)

Richard Wendl

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG

ZER10008.doc   Owner: SEN VA LP   Number of Declaration: 10 / 008

conformity in accordance with ISO/IEC 17050

6.2 BSIP1US DECT standard USA

- This device complies with Part 15 of the FCC rules and with RSS-210 of Industry Canada.

- Operation is subject to the following two conditions:

  1. this device may not cause harmful interference, and

  2. this device must accept any interference received, including interference that may cause undesired operation.

  3. Changes or modifications made to this equipment not expressly approved by (manufacturer name) may void the FCC authorization to operate this equipment.

- This device is tested and fulfills the Radio Standards Specification RSS-213 Issue 2.

- This device complies with FCC Part 15 Subpart D, unlicensed personal communication devices.

- Frequency band: 1920-1930 MHz.

- Type of Modulation: multi carrier time division multiple access with Digital modulation (GFSK).

- Number of channels: 5 RF Channels, 5x12=60TDMA Duplex channels.

- Antenna information: 2 permanent attached antennas, no external connector.

- RF Power: max. +20,5dBm.

- Temperature range: -10 to +45 degree Celsius (ambient).

- FCC ID: AY3-BSIP1US.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Radiofrequency radiation exposure Information:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

6.3 Base Stations

General

- Software   Can be loaded via the communication system.
- Antennas   Two external antennas are mounted on the top of the housing of the base station.
  The base station works with antenna diversity (this means that the radio receiver is connected to whichever antenna delivers the greater field strength).
- Average output power   10 mW to 125 mW
- Radio range   Basically dependant on the radio transmission characteristics of the environment/premises.
  - Outdoors   Up to 300 m
  - Indoors   Up to 50 m
- Power supply   PoE is used to supply power to the DECT IP base station
- Accessories   Outdoor housing

DECT IP Basisstation BSIP1

- Dimensions   202 x 172 x 43 (W x H x D in mm)
- Weight   500 g
- Power supply   PoE, according IEEE 802.3af Class 2
- Power consumption   < 6,5 W
- Operating temperature indoors + 0°C to + 40°C
  Outdoors (in outdoor housing) - 25°C to + 40°C
- Cabling   10/100 Mbps Ethernet cable, Cat. 5 and higher, 8-pin shielded RJ45 connector

LED status displays on the base station

- No settings need be made at the base station.

- LED 1/LED 2 on the front of the base station provides the following information:

Operating State	LED 1		LED 2	
LED status at booting sequence				
No power on Base station	off		off	
BSIP1 is booting the the Active partition	red flashing		red flashing	
BSIP1 is booting the the Fallback partition	red flashing		off	
BSIP1 is booting the Active partition with factory defaults	red fast flashing		red fast flashing	
BSIP1 is booting the Fallback partition with factory defaults	red fast flashing		off	
BSIP1 is booting kernel with Active partition	off		red	
BSIP1 is booting kernel with Fallback partition	red		off	
LED status at working process				
BSIP1 not ready Services not started or starting	orange		orange	
BSIP1 ready No LAN link	red		red	
BSIP1 ready No Connection to IWU	green		red	
BSIP1 ready All DECT-frequencies blocked or all available DECT channels occupied	red		green	
BSIP1 ready Link unsynchronized (DECT/LAN), no active call	off		green	

Table 8   LED status displays on the base station

Operating State	LED 1		LED 2	
BSIP1 ready Link unsynchronized (DECT/LAN), at least one active call *	off		green flashing	
BSIP1 ready Link synchronized (DECT/LAN), no active call	green		green	
BSIP1 ready Link synchronized (DECT/LAN), at least one active call	green		green flashing	

Table 8   *LED status displays on the base station*

*   On BSIP IWU means this LED status that a call might by located at another BSIP and be routed via the BSIP IWU

Blinking frequency = 500 msec. ON, 500 msec. OFF

LED 1 LED 2
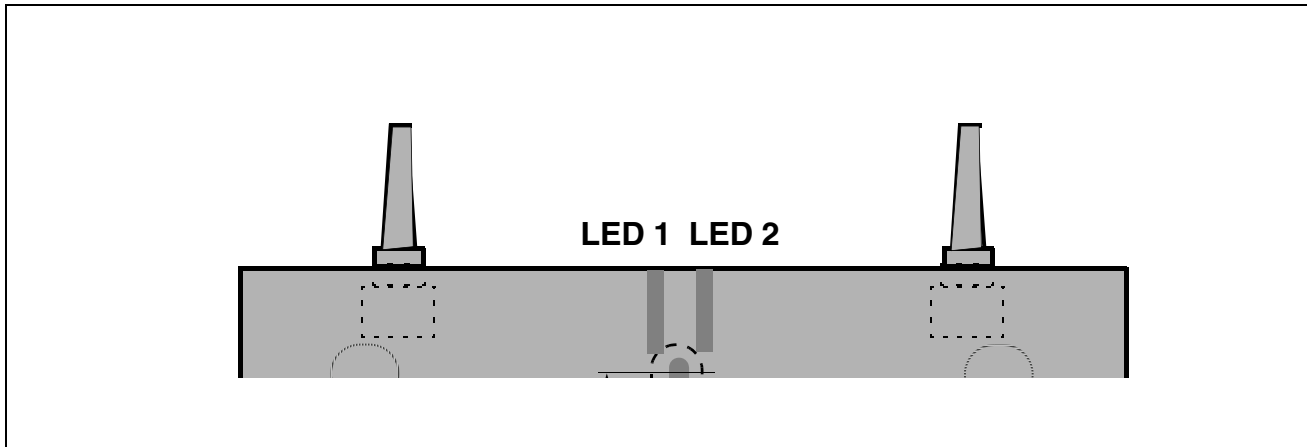
Figure 21   *LED position on the base station*

6.3.1 Mobile Telephones

All the mobile telephones mentioned in this section are suitable for use in normal environments. The Gigaset M2/M2*plus* and M2EX mobile telephones may also be used in industrial environments.

6.3.1.1 Gigaset S3 professional

• Software	Checking, see Section 7.2.2
• Output power	Average output power +10 dBm per channel Peak output power +24 dBm per channel
• Tone ringing	
– Volume control	adjustable 5 levels + crescendo ringing
– Tone ringing signal	Can be configured separately for internal and external calls (3 ringtones and 30 melodies)
• User Interface (UI)	Menu-driven graphic user interface
• Display	Illuminated color display
• Telephone book (integrated locally)	Up to a total of 250 entries
• Approved ambient conditions	+ 5°C to + 45°C 20% to 75% relative humidity
• Power supply (state of charge indicated on the display)	
– Recommended rechargeable batteries	**Nickel Metal Hydride (NiMH), 600 - 1200 mAh** Sanyo NiMH 800 GP 850 mAh Yuasa Technologies AAA 800

Do not remove batteries without good reason because charge state monitoring and the recharge function will not work properly if you do. After the batteries are removed and reinserted, they must be discharged and recharged as for the initial startup.

⚠️ **CAUTION**

The use of any other rechargeable batteries may cause functional disturbances or may damage the handsets. The manufacturer will not be held liable in such cases. If replacement batteries are required, be sure to use only the approved rechargeable types.

Example for a capacity of 800 mAh :

– Talktime	Up to 9 hours
– Standby time	Up to 175 hours
– Charging time in handset	approx. 9 h in charging unit, approx. 7 h in base station

The times for normal charging and initial charging are comparable.

• Housing	approx. 143 x 50 x 30 mm (L x W x H)
• Weight incl. rechargeable battery	approx. 119 g

Accessories

• Charging unit for EU including plug-in power supply unitt	S30852-H1980-R142
• Charging unit for UK including plug-in power supply unit	S30852-H1980-L142
• Charging unit for US including plug-in power supply unit	S30852-H1980-R142
• Charging unit for AUS including plug-in power supply unit	S30852-H1980-C442

NOTE: The home version of the Gigaset S3 professional will be classified by the HiPath Cordless IP system as GAP-device.

6.3.1.2 Gigaset SL3 professional

• Software	Checking, see Section 7.2.2
• Output power	Average output power +10 dBm per channel
	Peak output power +24 dBm per channel
• Tone ringing	
– Volume control	adjustable 5 levels + crescendo ringing
– Tone ringing signal	Can be configured separately for internal and external calls (3 ringtones and 30 melodies)
• User Interface (UI)	Menu-driven graphic user interface
• Display	Illuminated color display
• Telephone book (integrated locally)	Up to a total of 250 entries
• Approved ambient conditions	+ 5°C to + 45°C
	20% to 75% relative humidity
• Power supply (state of charge indicated on the display)	
• Approved battery pack	**Lithium-Ion (Li-Ion), 700 mAh**

Do not remove the battery pack without good reason as charge state monitoring and the recharge function will not work properly if you do! After the batteriey pack is removed and reinserted, it must be discharged and recharged as for the initial startup!

⚠ **CAUTION**

The use of any other battery packs may cause functional disturbances or may damage the handsets. The manufacturer will not be held liable in such cases. If replacement battery packs are required, be sure to use only the approved types.

– Talktime	Up to 14 hours
– Standby time	Up to 350 hours
– Charging time in handset	approx. 3,5 h

The times for normal charging and initial charging are comparable.

• Housing	approx. 114 x 46,5 x 22,6 mm (L x W x H)
• Weight incl. battery pack	approx. 93 g

Accessories

- Charging unit for EU including plug-in power supply unit S30852-H1982-R141
- Charging unit for UK including plug-in power supply unit S30852-H1982-L141
- Charging unit for US including plug-in power supply unit S30852-H1982-U141
- Charging unit for AUS including plug-in power supply S30852-H1982-C441
  unit

NOTE: The home version of the Gigaset SL3 professional will be classified by the HiPath Cordless IP system as GAP-device.

6.3.1.3 Gigaset M2 professional, Gigaset M2 *plus* professional

• Software	Checking, see Section 7.2.2
• Output power	Average output power +10 dBm per channel Peak output power +24 dBm per channel
• Tone ringing	
– Volume control	adjustable: 5 levels, levels 4 and 5 for loud environments.
– Tone ringing signal	Can be configured separately for internal and external calls 20 standard ringtones (3 ringtones / 17 melodies) 16 loadable polyphonic melodies
• User Interface (UI)	Menu-driven graphic user interface
• Display	Illuminated color display
• Telephone book (integrated locally)	Up to a total of 250 entries
• Voice dialing (voice telephone book)	Up to 30 entries
• Full functionality of device guaranteed for	-10 °C to +55 °C 100 % relative humidity including splashes and low pressure jets of water (IP 65)
• Power supply (state of charge indicated on the display)	
• Approved battery pack	**Lithium-Ion, 1000 mAh (A5B00075416005)**

Do not remove the battery pack without good reason as charge state monitoring and the recharge function will not work properly if you do! After the batteriey pack is removed and reinserted, it must be discharged and recharged as for the initial startup!

⚠ **CAUTION**

The use of any other battery packs may cause functional disturbances or may damage the handsets. The manufacturer will not be held liable in such cases. If replacement battery packs are required, be sure to use only the approved types.

Example for a capacity of 850 mAh:

– Talktime	Up to 12 hours
– Standby-Time	Up to 380 hours, approx. 16 days
– Charging time in handset	approx. 3,7 hours
– Initial charging time	at least 10 h
• Housing	approx. 166,5 x 56,0 x 35,4 mm (L x W x H)
• Weight incl. battery pack	approx. 180 g

Accessories

- Charging unit for EU including plug-in power supply unit S30852-H1786-R101
- Charging unit for UK including plug-in power supply unit S30852-H1786-L101

6.3.1.4 Gigaset M2 Ex professional

• Software	Checking, see Section 7.2.2
• Output power	Average output power +10 dBm per channel Peak output power +24 dBm per channel
• Tone ringing	
– Volume control	adjustable: 5 levels, levels 4 and 5 for loud environments.
– Tone ringing signal	Can be configured separately for internal and external calls 20 standard ringtones (3 ringtones / 17 melodies) 16 loadable polyphonic melodies
• User Interface (UI)	Menu-driven graphic user interface
• Display	Illuminated color display
• Telephone book (integrated locally)	Up to a total of 250 entries
• Voice dialing (voice telephone book)	Up to 30 entries
• Full functionality of device guaranteed for	-10 °C to +55 °C 100 % relative humidity including splashes and low pressure jets of water (IP 65)
• Power supply (state of charge indicated on the display)	
– Permitted Ex-battery pack	**Lithium-Ion, 1000 mAh including electronic components (A5B00075609027)**

Do not remove the Ex-battery pack without good reason as charge state monitoring and the recharge function will not work properly if you do! After the Ex-battery pack is removed and reinserted, it must be discharged and recharged as for the initial startup!

⚠️ **CAUTION**

Only use approved Ex battery packs . Ex authorisation is only valid and the handset can only be operated if this battery pack is installed. Other battery packs are strictly prohibited. If they are used, Ex protection is no longer valid.

Example for a capacity of 850 mAh:

– Talktime	Up to 12 hours

– Standby-time	Up to 380 hours, approx. 16 days
– Charging time	approx. 3,7 h
– Initial charging time	at least 10 h
• Housing	approx. 166,5 x 56,0 x 35,4 mm (L x W x H)
• Weight incl. battery pack	approx. 180 g

Accessories

• Charging unit for EU including plug-in power supply unit	S30852-H1786-R101
• Charging unit for UK including plug-in power supply unit	S30852-H1786-L101

6.3.2 HiPath Cordless IP server

• FSC server with special HW-optimized Linux operating system (openWRT),

• Server is included in the scope of the solution (not a standard server).

Model	Fujitsu-Siemens, Floorstand, incl. 3.5" FD
Processor	Xeon UP X3220 2.40GHz 2x4MB 1066MHz Quad Core CPU with cooling element (95W) 2x4MB SLC ECC protected, 1066MHz FSB 64-bit/Intel® VT
RAM	1GB DDR2-800 PC2-6400 ub d ECC 1 module 1GB, unbuffered dual rank DDR2 8 no Chipkill
DVD drive	DVD-ROM 1.6" SATA 16x DVD, 48x CD 1.6" anthracite
Hard disk	HD SATA 3GB/s 250 GB 7.2k hot plug 3.5"
Miscellaneous	KBPC SX D standard keyboard global design bright light gray keyboard 2m PS2 Cable Mains supply line (D,..), 1.8 m, gray suitable for D, A, B, F, NL, FIN, N, E, P, RUS, TR
Optional available	Conversion kit for switching HiPath Cordless IP servers into 19-inch models (5 U)

Table 9　　　　　　　*HiPath Cordless IP server*

6.3.3 PoE Injector

• An injector is needed when operating the DECT IP base station on the mains,

• Single-port PoE injector in compliance with IEEE 802.3af Class 2

- Injector is included in the scope of features

- The PoE injector ships with startup information and notes on LED status displays.

6.4 Item Number Overview

- Base stations

  - HiPath Cordless IP V1 - Base station BSIP1   S30807-U5494-X

  - HiPath Cordless IP V1 - SW License per HiPath Cordless IP Server[*]   F31505-K111-A2

  - HiPath Cordless IP V1 - SW License per DECT IP Basisstation BSIP1*   F31505-K111-A1

  - HiPath Cordless IP V1 - CD-ROM with software   P30152-P1440-P1

  - DECT system number (ARI = Access Right Identifier)   A31003-G2121-S500-*-20

  - HiPath Cordless IP V1 - HiPath Cordless IP Server   CUZ:1265V101-SEN04 (to be ordered at Fujitsu)

  - One-Port PoE Injector   S30122-X8009-X20

  - Outdoor mounting   S30122-X7469-X2

  - Power line for PoE injector - EU   C39195-Z7001-C11

  - Power line for PoE injector - UK   C39195-Z7001-C20

  - Power line for PoE injector - Switzerland   C39195-Z7001-C38

  *only needed if the HiPath Cordless IP server software is installed on dedicated server hardware and not on one of the DECT IP base stations

- Terminals

  - **Gigaset M2 professional**   S30852-S1756-R111

  - Charging unit for EU including plug-in power supply unit   S30852-H1786-R101

  - Charging unit for UK including plug-in power supply unit   S30852-H1786-L101

  - **Gigaset M2 EX professional**   S30852-S1756-R121

  - Charging unit for EU including plug-in power supply unit   S30852-H1786-R101

  - Charging unit for UKincluding plug-in power supply unit   S30852-H1786-L101

  - **Gigaset M2 *plus* professional**   S30852-S1756-R131

  - Charging unit for EU including plug-in power supply unit   S30852-H1786-R101

  - Charging unit for UK including plug-in power supply unit   S30852-H1786-L101

  - **Gigaset S3 professional**   S30852-H1950-R142

  - Charging unit for EU including plug-in power supply unit   S30852-H1980-R142

  - Charging unit for UK including plug-in power supply unit   S30852-H1980-L142

  - Charging unit for US including plug-in power supply unit   S30852-H1980-R342

  - Charging unit for AUS including plug-in power supply unit   S30852-H1980-C442

  - **Gigaset SL3 professional**   S30852-H1952-R142

  - Charging unit for EU including plug-in power supply unit   S30852-H1982-R141

  - Charging unit for UK including plug-in power supply unit   S30852-H1982-L141

  - Charging unit for US including plug-in power supply unit   S30852-H1982-U141

– Charging unit for AUS including plug-in power supply   S30852-H1982-C441
unit

*

6.5 Measuring Equipment

- HiPath Cordless Servicetool HCS DECT   TIS
Locater / Locater Pro   Technische Informations-Systeme GmbH
Barloer Weg 190
46397 Bocholt, Germany
Tel.: (0 28 71) 27 22 - 0, (0 28 71) 3 78 62
http://www.tis-gmbh.de/produkte/

6.6 Operating Manuals

See http://apps.g-dms.com:8081/techdoc/search_en.htm

7 Diagnosis and Maintenance

7.1 Checking the Base Stations and the Radio Coverage

Do not use Gigaset mobile telephones to check the radio area coverage. This must be done with the Hicom Cordless Service tool (HCS-DECT).

You can use Gigaset mobile telephones to test the base stations and verify the radio area coverage.

- A prerequisite is that the mobile telephone being used is logged on to the system, see the operating manual.

- The radio coverage is tested in two stages:

  - Base station test

  - Coverage test via the base stations (area coverage)

The following minimum values must be observed for the site survey of the radio range:

  1. Providing handsets with an adequate DECT radio signal

Handsets only receive a sufficiently sized DECT radio signal if they are located in the radio range of the DECT IP base station, that is:

  - RSSI value <-70 dBm

  - FRAQ value >95%

  2. Distance of DECT IP base stations

For the DECT synchronism function to work, the DECT IP base stations to be synchronized with each other must be defined in the HiPath Cordless IP server software. These DECT IP base stations must also be able to exchange their management information, i.e. they must be at least <-85 dBm apart.

Failure to maintain these values results in a loss of radio signal or a loss of synchronism which prevents the handsets from roaming to another DECT IP base station.

7.1.1 Base Stations

The purpose of this test is to check the functions of all base stations.

- Take the mobile telephone to each of the base stations.

- Holding the mobile telephone directly below, beside or above each base station, turn it off and on again.

  – Display data, for example:

Synchronization between mobile telephone and base station	Base n	Radio connection to the base station is displayed on the screen as "Base n", for example.
No synchronization between mobile telephone and base station	Base n	"Base n" flashes, it means that the radio connection to the base station has been lost.
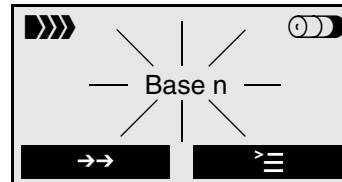
- Set the mobile telephone to measuring mode.

NOTE: Values recorded with a mobile telephone are not very precise and are intended to provide a rough assessment only. In addition, different values may be recorded on each mobile telephone even though the ambient conditions are identical. If you require more accurate results, we recommended that you use the Hicom Cordless Service tool (HCS-DECT).

Check:

  – **RSSI value** (field strength value)

  – **RPN value** (base station number)
    Does the mobile telephone pick up the connection (synchronization) with the base station to be tested?

  – **FRAQ value** (transmission quality %)

If the indicated values are not attained, use a second logged-on mobile telephone to check the value ranges.
If the indicated values are not attained with the second mobile telephone, replace the base station.

⚠ **WARNING**

The customer must be informed about the boundaries of the radio area.

Proceed with the area coverage test once the RSSI value, the availability and radio quality of all base stations has been checked.

7.1.2 Quick Verification of Area Coverage

The purpose of this test is to check whether the necessary field strength and the transmission quality is attained throughout the entire radio network.

NOTE: Values recorded with a mobile telephone are not very precise and are intended to provide a rough assessment only. In addition, different values may be recorded on each mobile telephone even though the ambient conditions are identical. If you require more accurate results, we recommended that you use the Hicom Cordless Service tool (HCS-DECT).

Step 1

The purpose of this step is to provide the basis for step 2 where you will use a Gigaset mobile telephone to obtain a rough assessment of the area coverage.

• Switch the mobile telephone to measuring mode (see Section 7.2.2.1).

• Establish a voice connection between two mobile telephones. If you wish, you can use an announcement service (for example "speaking clock").

Step 2

This step involves obtaining a rough assessment of the area coverage.

• With a mobile telephone in measuring mode, move around the area in question and determine whether an RSSI value > 50 (-60 dBm) and a FRAQ value > 95% are reached throughout the area.
In the process, the Range Warning feature can be used as an aid for recognizing the radio area boundaries. A warning tone (range warning) is

emitted as soon as you cross the border zone of the radio area. (To activate the range warning tone, use the "Tones" menu on the mobile telephone display.)

⚠ **WARNING**

Areas in the corners of buildings or behind metal structures should be carefully checked (check the RSSI values several times).

In these radio area border zones, the radio connection to the base station may be lost in the case of the following values:

RSSI	< 40 (< -80 dBm)
FRAQ	< 95%

• The measuring sites with RSSI value < 40 (< -80 dBm) should be entered or marked in the building/site plan.

Step 3

If you require more accurate values than those obtained in step 2, we recommended that you use the Hicom Cordless Service tool (HCS-DECT).

7.2 Testing the Radio Area

7.2.1 Significance of Results Obtained

NOTE: Values recorded with a mobile telephone are not very precise and are intended to provide a rough assessment only. In addition, different values may be recorded on each mobile telephone even though the ambient conditions are identical. If you require more accurate results, we recommended that you use the Hicom Cordless Service tool (HCS-DECT)

The following figure shows a sample display of the measuring results for a Gigaset mobile telephone when a call is in progress:

Measurement result

RSSI (radio signal)	Field strength of the radio signals received from the base station, normalized to a maximum of 100. If the value is < 50, the radio connection to the base station is no longer guaranteed. Acceptable field strength is > 50 (> -60 dBm).
Frequency	Frequency (0 – 9)
Time slot (Slot)	Time slot (0 – 11) of the receiving channel on which the measurement is carried out.
RPN (port number)	IDECT IP base station identification based on the RPN (Radio Fixed Part Number), e.g. 018. If the handset switches on at/over to an overlapping radio cell/DECT IP base station, the current DECT IP base station appears on the handset display. The RPN is indicated in hex format in Gigaset S3 professional and Gigaset SL3 professional handsets.
	Example: RPN 018 will be display in the Gigasets as HEX-value 012H. The identifier "H" shows clearly the hexadecimal presentation.
FRAQ (frame quality)	Transmission quality in %. 95 % to 100 % satisfactory (for short periods 90 % to 94 % non-critical), < 95 % faulty.

7.2.2 Gigaset Family

NOTE: The default language for measuring mode is English.

7.2.2.1 Activating Measuring Mode

You must switch off the mobile telephone before you can activate measuring mode.

Switch off the mobile telephone:

Nothing is displayed

Press the on-hook key until the confirmation beep is heard (ascending tone sequence).

Switch the mobile telephone into service status:

1	2	3
4	5	6
7	8	9
*	0	#

Press keys 1, 4, and 7 simultaneously...

... whilst at the same time...

... pressing the on-hook key.

Service

Activate the "Service" menu:

1	2	3
4	5	6
7	8	9
*	0	#

Enter code 76200.
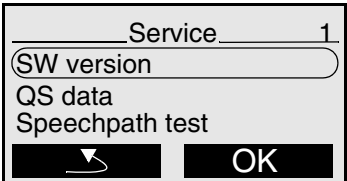
Service   1
(SW version)
QS data
Speechpath test

OK

Activate the measuring mode:

Using the navigation key, scroll down to "Measuring time".
Confirm with OK.
Measuring mode is switched on; this is indicated by the tick next to "Measuring mode".

```
_____Service_____6
DSP parameters
(Measuring mode          ✓)
Measuring time
    ↘              OK
```
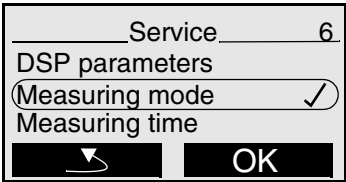
Select the measuring time:

Using the navigation key, scroll down to "Measuring time".
Confirm with OK.

```
_____Service_____7
Measuring mode           ✓
(Measuring time           )
LLLLLLLLLLLLLLL
    ↘              OK
```
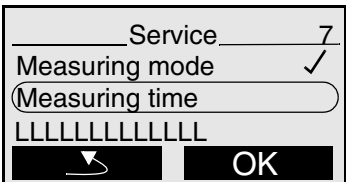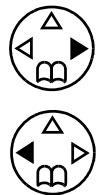
Set the value range:

Press the navigation key:
to increase the value range

Press the navigation key:
to reduce the value range

Value range: 06 to 16
Recommended value range: 16
(measuring cycle: 1 s to 2.5 s)

```
____Measuring time____
Measuring time      <16>


    ↘            Save
```
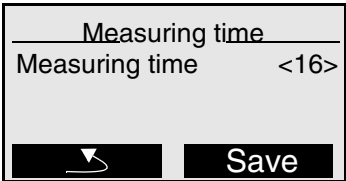
Save

Press the Save key
to confirm the value range set

Switch off the mobile telephone:

Press the on-hook key until the confirmation beep is heard (ascending tone sequence).

Nothing is displayed
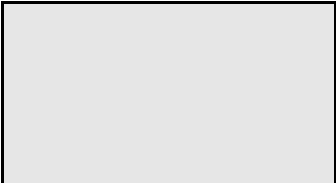
The measurement values are displayed when the mobile telephone is switched on. Measurements are performed at the set intervals (see Section 7.2.1).

Switch on the mobile telephone:

Press the on-hook key until the confirmation beep is heard (ascending tone sequence).

095-3-02-012H-100

*Base n

→→   ≥☰
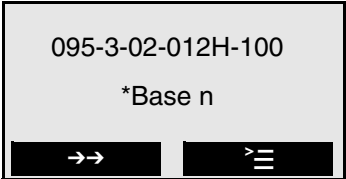
⚠ **WARNING**

Only the specified functions may be activated. Activating other functions may result in malfunctions.

7.2.2.2 Deactivating Measuring Mode

Switch off the mobile telephone:

Nothing is displayed

Press the on-hook key until the confirmation beep is heard (ascending tone sequence).

Switch the mobile telephone into service status:

1	2	3
4	5	6
7	8	9
*	0	#

Press keys 1, 4, and 7 simultaneously...

... whilst at the same time...

... pressing the on-hook key.

Service

Activate the "Service" menu:

Enter code 76200.

1	2	3
4	5	6
7	8	9
*	0	#

```
_____Service_____1_
(SW version                )
QS data
Speechpath test
[    ↘    ] [    OK    ]
```

Deactivate the measuring mode:

Using the navigation key, scroll down to "Measuring time".
Confirm with OK.
Measuring mode is switched off; the tick next to "Measuring mode" disappears.

OK

```
_____Service_____6_
DSP parameters
(Measuring mode            )
Measuring time
[    ↘    ] [    OK    ]
```

Switch off the mobile telephone:

Nothing is displayed

Press the on-hook key until the confirmation beep is heard (ascending tone sequence).

The measurement values are not displayed if the mobile telephone is switched on.

7.2.3 Documentation of Results

The following points must be documented:

*   The installation site of the base stations must be drawn on a customer-specific building/site plan and the base station number (for example, 016 (RPN in measuring mode)) entered.

*   Any deviations from existing building and site plans must be verified with the Hicom Cordless Service tool (HCS-DECT) and documented.

⚠ **WARNING**

Any subsequent structural changes within the radio area (buildings, sites, facilities, and devices, etc.) might restrict the operation of the mobile telephones and thus require rearrangement of the base stations.

Examples:
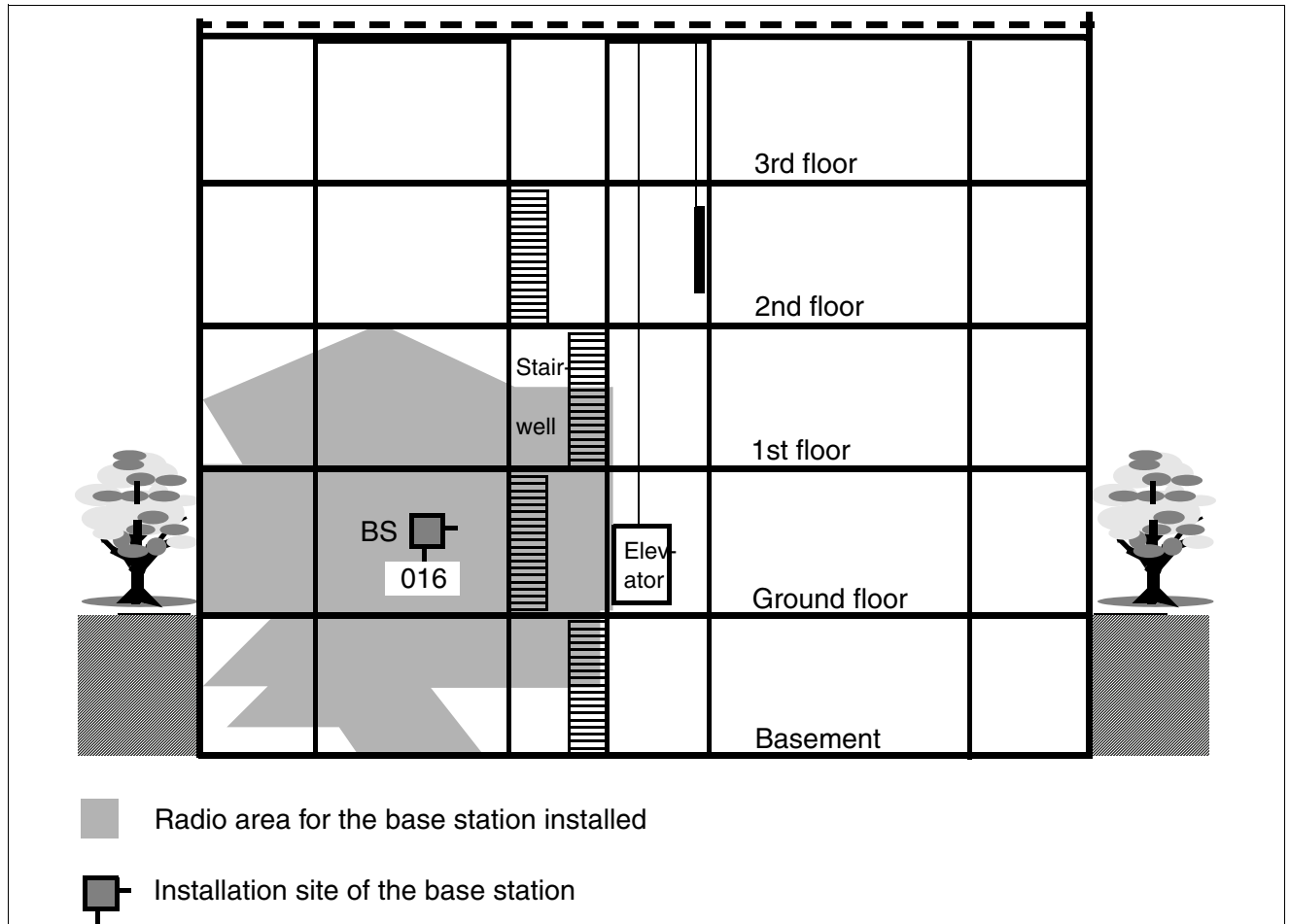
Figure 23   Building - Base station installation site/radio area
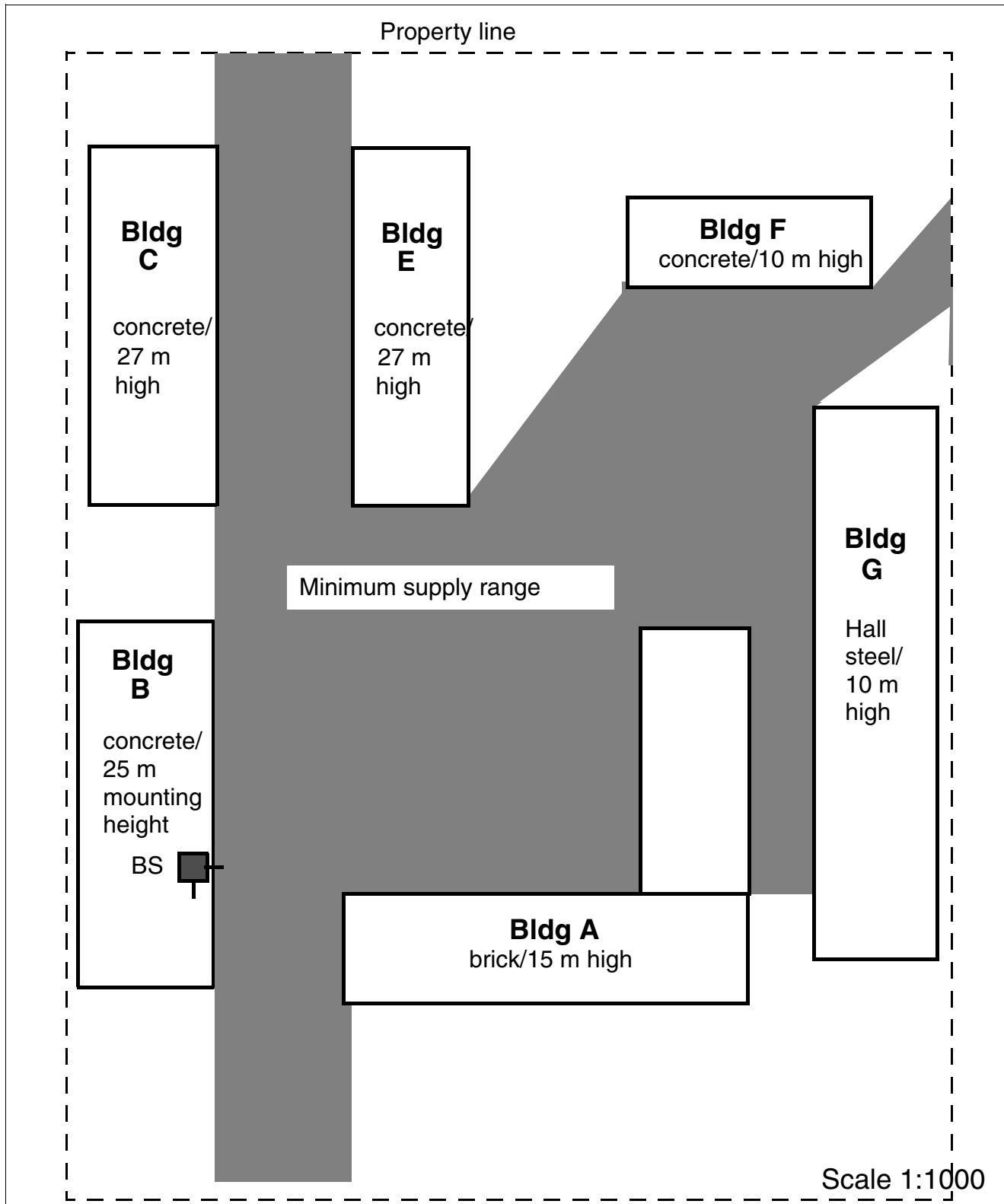
Figure 24   *Outdoors - Base station installation site/radio area*

7.3 Troubleshooting

7.3.1 Checking HiPath Cordless IP Components

- Entire system

  - Set up call with the   Operating Manual
    mobile telephone   Subjective evaluation of voice connection, for example,
                               background noise

- Check the radio area   See Section 7.1.2
   coverage   (range warning tone activated)

- DECT IP Base station
  (BSIP1)

  - LED 1/2   See Section 6.3

  - Base station status   PC

  - Check active status of   **No synchronism:**
    base station using the   "Base n" blinks on handset display.
    logged-on mobile   **Handset measuring mode is activated:**
    telephone   - Frequency/slot changes
                               - RSSI value
                               If this is not the case, perform the test on a different base
                               station.
                               If it is still unsuccessful, use a different handset.
                               If it is still not possible to synchronize with a base station
                               after repeated attempts, replace the base station.

- Mobile telephone (MT)

  - Logged-on mobile   Synchronism symbol "Base n" (name = individual
    telephone, synchronized   setting) on handset display is continuously visible, does
    with base station   not blink.

7.3.2 What Happens If ...

7.3.2.1 Synchronism Symbol on Handset Display:

– "Base n" flashes	**No synchronization** to base station

1. Is the mobile telephone not logged on?

2. If the mobile telephone is logged on to multiple systems, is it switched to the correct system? Is automatic system selection activated?
    Check the base station.

– "Base n" continuously visible but no action is possible	**Synchronization** to base station

1. An error tone can be heard when the line key is pressed.
    Temporary overload status (all the base station speech paths are busy).

    Wait, and try again.

2. Handset was not able to complete the locations request successfully (handset contact to the system).

    Workaround:

    Repeat locations request by switching off the handset and then switching it on again.

7.3.2.2 Handset Cannot Be Reached

1. Handset is called, caller hears ringing (followed by busy signal).

   Causes:
   handset being called is switched off
   OR
   handset is no longer within range
   OR
   the base station used is in overload status and there is no other base station within range.

2. Handset is called, call is always switched to another station.
   Handset has inadvertently activated call forwarding.

7.3.2.3 Connection Handover

– Call disconnected on handover to another base station

1. Check whether or not the base station to which the call is handed over is in overload status (all radio channels busy).

2. Check the base station LEDs.

3. Check the overlap sectors.
   Is the RSSI value of the other base station OK?

4. Check if the two DECT IP base stations involved in the handover operation are synchronous. You can use the Gigaset's measurement mode for this or the synchronism display in the HiPath Cordless IP server software .

7.3.2.4 Handset: Problems Logging On

• Check first if the communication server's IP board and at least one DECT IP base station (in range) are operational.

• Is adequate synchronism guaranteed for the DECT IP base station in the HiPath Cordless IP system?

• Is the handset you want to log on configured on the communication server?

– Test this with a random phone (optiPoint/OpenStage model).

8 Open Source Software used in the Product

8.1 General Conditions

The Product "HiPath Cordless IP" contains, among other things, Open Source Software, licensed under an Open Source Software License and developed by third parties. These Open Source Software files are protected by copyright. Your rights to use the Open Source Software beyond the mere execution of Siemens´ program, is governed by the relevant Open Source Software li-cense conditions.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between Siemens Enterprise Communication GmbH&Co. KG license conditions and the Open Source Software license conditions, the Open Source Software conditions shall prevail with respect to the Open Source Software por-tions of the software. The Open Source Software is licensed royalty-free (i.e., no fees are charged for exercising the licensed rights, whereas fees may be charged for reimbursement of costs incurred by Siemens Enterprise Communication GmbH&Co. KG. The license conditions can be found in the following chapters. In addition the license texts can be downloaded from:

- The BSD License is available on the internet at:

  http://www.freebsd.org/copyright/license.html

- The GPL v2 is available on the internet at:

  http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

- The LGPL v2.1 is available on the internet at:

  http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

- The OpenSSL license is available on the internet at:

  http://www.openssl.org/source/license.html

- The zLib license is available on the internet at:

  http://www.zlib.net/zlib_license.html

- The c-ares license is available on the internet at:

  http://c-ares.haxx.se/license.html

If programs contained in this product are licensed under GNU General Public License (GPL) and/or GNU Lesser General Public License (LGPL) and this software is not already delivered in source code form together with the device, you can request the corresponding source code from Siemens Enterprise Communication GmbH&Co. KG by paying a fee of 10 Euro for the physical act of transferring the copy.

Open Source Software used in the Product
General Conditions

Please send your specific request, together with a receipt indicating the date of purchase, within three years of your purchase, together with the MAC ID number of the device and the software release number to:

Your local Service Organisation of Siemens Enterprise Communication GmbH&Co. KG

Warranty regarding further use of the Open Source Software:

Siemens Enterprise Communication GmbH&Co. KG provides no warranty for the Open Source Software programs contained in this device, if such programs are used in any manner other than the program execution intended by Siemens Enterprise Communication GmbH&Co. KG. The li-censes listed below define the warranty, if any, from the authors or licensors of the Open Source Software. Siemens Enterprise Communication GmbH&Co. KG specifically disclaims any warran-ties for defects caused by altering any Open Source Software program or the product's configu-ration. You have no warranty claims against Siemens Enterprise Communication GmbH&Co. KG in the event that the Open Source Software infringes the intellectual property rights of a third party.

Technical support, if any, will only be provided for unmodified software.

8.2   Open Source Software Used

Open Source Software Component	License
U-Boot	GPLv2
Busybox	GPLv2
binutils	GPLv2
ethtool	GPLv2
hotplug2	GPLv2
ipsec-tools	X11-License, 3-clause BSD
libelf	LGPLv2.1
libpcap	BSD License
iptables	GPLv2
lsof	lsof License
mini_httpd	BCD License 2 clause
libpcap	BCD License
net-snmp	BSD Licenses
openSSL	OpenSSL License, SSLeay License
ntp	Ntp, without GPLv2 parts
strace	BCD License
tcpdump	BCD License
mtd-utils	GPLv2
gcc 4.* incl. libstdc++	GPLv2
zlib	Zlib-license
openSSH	BSD Licenses, MIT License
dropbear	BSD Licenses
uClibc incl. libpthread	LGPLv2.1
linux kernel 2.6.2x	GPLv2
JSON-C	X11
alsa-lib-1.0.13	LGPLv2.1
bridge-utils-1.4	GPLv2
c-ares-1.7.4	MIT-License
e2fsprogs-1.39	GPLv2/BSD-style
file-4.19	BSD-styple

Open Source Software Component	License
gdbserver-6.8	GPLv2
grub-0.97	GPLv2
libiconv-1.9.1	LGPLv2.1/iconv GPLv2
libusb-0.1.12	LGPL und BSD license
Linux-PAM-0.99.6.3	GPLv2, distributable
ncurses-5.6	GPLv2, X11/MIT
pciutils-2.2.9	GPLv2
procps-3.2.7	GPLv2
readline-5.1	GPLv2
udev-106	GPLv2
util-linux-2.12r	BSD 3-Clause, GPL v2 or later

8.3   Acknowledgements

OpenSSL:

- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

Zlib:

- This product includes software developed by Jean-loup Gailly and Mark Adler

Libpcap:

- This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

8.4   Text of the used Open Source Software Licenses

8.4.1   GPL

```
                GNU GENERAL PUBLIC LICENSE
                  Version 2, June 1991
```

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

                        Preamble

The licenses for most software are designed to take away your freedom to share
and change it. By contrast, the GNU General Public License is intended to
guarantee your freedom to share and change free software--to make sure the
software is free for all its users. This General Public License applies to
most of the Free Software Foundation's software and to any other program whose
authors commit to using it. (Some other Free Software Foundation software
is covered by the GNU Library General Public License instead.) You can apply
it to your programs, too.

  When we speak of free software, we are referring to freedom, not price.
Our General Public Licenses are designed to make sure that you have the free-
dom to distribute copies of free software (and charge for this service if you
wish), that you receive source code or can get it if you want it, that you
can change the software or use pieces of it in new free programs; and that
you know you can do these things.

 To protect your rights, we need to make restrictions that forbid anyone to
deny you these rights or to ask you to surrender the rights. These restric-
tions translate to certain responsibilities for you if you distribute copies
of the software, or if you modify it.

 For example, if you distribute copies of such a program, whether gratis or
for a fee, you must give the recipients all the rights that you have. You
must make sure that they, too, receive or can get the source code. And you
must show them these terms so they know their rights.

 We protect your rights with two steps: (1) copyright the software, and (2)
offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

```
                    GNU GENERAL PUBLIC LICENSE

    TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION
```

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to
give any third party, for a charge no more than your cost of physically per-
forming source distribution, a complete machine-readable copy of the corre-
sponding source code, to be distributed under the terms of Sections 1 and 2
above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to
distribute corresponding source code. (This alternative is allowed only for
noncommercial distribution and only if you received the program in object
code or executable form with such an offer, in accord with Subsection b
above.)

The source code for a work means the preferred form of the work for making
modifications to it. For an executable work, complete source code means all
the source code for all modules it contains, plus any associated interface
definition files, plus the scripts used to control compilation and installa-
tion of the executable. However, as a special exception, the source code
distributed need not include anything that is normally distributed (in either
source or binary form) with the major components (compiler, kernel, and so
on) of the operating system on which the executable runs, unless that compo-
nent itself accompanies the executable.

If distribution of executable or object code is made by offering access to
copy from a designated place, then offering equivalent access to copy the
source code from the same place counts as distribution of the source code,
even though third parties are not compelled to copy the source along with the
object code.

   4. You may not copy, modify, sublicense, or distribute the Program except
as expressly provided under this License. Any attempt otherwise to copy,
modify, sublicense or distribute the Program is void, and will automatically
terminate your rights under this License.

However, parties who have received copies, or rights, from you under this
License will not have their licenses terminated so long as such parties remain
in full compliance.

   5. You are not required to accept this License, since you have not signed
it. However, nothing else grants you permission to modify or distribute the
Program or its derivative works. These actions are prohibited by law if you
do not accept this License. Therefore, by modifying or distributing the Pro-
gram (or any work based on the Program), you indicate your acceptance of this
License to do so, and all its terms and conditions for copying, distributing
or modifying the Program or works based on it.

   6. Each time you redistribute the Program (or any work based on the Pro-
gram), the recipient automatically receives a license from the original li-
censor to copy, distribute or modify the Program subject to these terms and
conditions. You may not impose any further restrictions on the recipients'
exercise of the rights granted herein. You are not responsible for enforcing
compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent in-
fringement or for any other reason (not limited to patent issues), conditions
are imposed on you (whether by court order, agreement or otherwise) that con-
tradict the conditions of this License, they do not excuse you from the con-
ditions of this License. If you cannot distribute so as to satisfy simulta-
neously your obligations under this License and any other pertinent
obligations, then as a consequence you may not distribute the Program at all.
For example, if a patent license would not permit royalty-free redistribution
of the Program by all those who receive copies directly or indirectly through
you, then the only way you could satisfy both it and this License would be
to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply and
the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents
or other property right claims or to contest validity of any such claims;
this section has the sole purpose of protecting the integrity of the free
software distribution system, which is implemented by public license prac-
tices. Many people have made generous contributions to the wide range of
software distributed through that system in reliance on consistent applica-
tion of that system; it is up to the author/donor to decide if he or she is
willing to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to be a
consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain
countries either by patents or by copyrighted interfaces, the original copy-
right holder who places the Program under this License may add an explicit
geographical distribution limitation excluding those countries, so that dis-
tribution is permitted only in or among countries not thus excluded. In such
case, this License incorporates the limitation as if written in the body of
this License.

9. The Free Software Foundation may publish revised and/or new versions of
the General Public License from time to time. Such new versions will be
similar in spirit to the present version, but may differ in detail to address
new problems or concerns.

Each version is given a distinguishing version number. If the Program spec-
ifies a version number of this License which applies to it and "any later
version", you have the option of following the terms and conditions either
of that version or of any later version published by the Free Software Foun-
dation. If the Program does not specify a version number of this License,
you may choose any version ever published by the Free Software Foundation.

   10. If you wish to incorporate parts of the Program into other free programs
whose distribution conditions are different, write to the author to ask for
permission. For software which is copyrighted by the Free Software Founda-
tion, write to the Free Software Foundation; we sometimes make exceptions for
this. Our decision will be guided by the two goals of preserving the free
status of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

                           NO WARRANTY

   11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTH-
ERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE
THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND
PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE,
YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

   12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDIS-
TRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUD-
ING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF
THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS
OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD
PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.

                    END OF TERMS AND CONDITIONS

    How to Apply These Terms to Your New Programs

  If you develop a new program, and you want it to be of the greatest possible
use to the public, the best way to achieve this is to make it free software
which everyone can redistribute and change under these terms.

   To do so, attach the following notices to the program. It is safest to
attach them to the start of each source file to most effectively convey the
exclusion of warranty; and each file should have at least the "copyright"
line and a pointer to where the full notice is found.

    <one line to give the program's name and a brief idea of what it
    does.> Copyright (C) <year> <name of author>

   This program is free software; you can redistribute it and/or modify
   it under the terms of the GNU General Public License as published by
   the Free Software Foundation; either version 2 of the License, or
   (at your option) any later version.

        This program is distributed in the hope that it will be useful,
        but WITHOUT ANY WARRANTY; without even the implied warranty of
        MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
        GNU General Public License for more details.

        You should have received a copy of the GNU General Public License
        along with this program; if not, write to the Free Software
        Foundation, Inc., 59 Temple Place, Suite 330, Boston,
        MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when
it starts in an interactive mode:

        Gnomovision version 69, Copyright (C) year name of author'
        Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type
        `show w'.
        This is free software, and you are welcome to redistribute it
        under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may be
called something other than `show w' and `show c'; they could even be mouse-
clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if neces-
sary. Here is a sample; alter the names:

        Yoyodyne, Inc., hereby disclaims all copyright interest in the
        program `Gnomovision' (which makes passes at compilers) written by
        James Hacker.

        <signature of Ty Coon>, 1 April 1989
        Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may con-
sider it more useful to permit linking proprietary applications with the li-
brary. If this is what you want to do, use the GNU Library General

Public License instead of this License.

8.4.2　LGPL

```
             GNU LESSER GENERAL PUBLIC LICENSE

                Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

    59 Temple Place, Suite 330, Boston, MA  02111-1307  USA

 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.
```

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

```
                        Preamble
```

  The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

  This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

  When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

  To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

  For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

    a) The modified work must itself be a software library.

    b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

    c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

    d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

    (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

  3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

  Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

  This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

  4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

  If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

  5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates
an executable that is a derivative of the Library (because it contains por-
tions of the Library), rather than a "work that uses the library". The ex-
ecutable is therefore covered by this License. Section 6 states terms for
distribution of such executables.

When a "work that uses the Library" uses material from a header file that
is part of the Library, the object code for the work may be a derivative work
of the Library even though the source code is not. Whether this is true is
especially significant if the work can be linked without the Library, or if
the work is itself a library. The threshold for this to be true is not pre-
cisely defined by law.

If such an object file uses only numerical parameters, data structure lay-
outs and accessors, and small macros and small inline functions (ten lines
or less in length), then the use of the object file is unrestricted, regard-
less of whether it is legally a derivative work. (Executables containing
this object code plus portions of the Library will still fall under Section
6.)

Otherwise, if the work is a derivative of the Library, you may distribute
the object code for the work under the terms of Section 6. Any executables
containing that work also fall under Section 6, whether or not they are linked
directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a
"work that uses the Library" with the Library to produce a work containing
portions of the Library, and distribute that work under terms of your choice,
provided that the terms permit modification of the work for the customer's
own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library
is used in it and that the Library and its use are covered by this License.
You must supply a copy of this License. If the work during execution displays
copyright notices, you must include the copyright notice for the Library
among them, as well as a reference directing the user to the copy of this
License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable
source code for the Library including whatever changes were used in the work
(which must be distributed under Sections 1 and 2 above); and, if the work
is an executable linked with the Library, with the complete machine-readable
"work that uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified executable
containing the modified Library. (It is understood that the user who changes
the contents of definitions files in the Library will not necessarily be able
to recompile the application to use the modified definitions.)

   b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

   c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

   d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

   e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

   For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

   7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

   8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void,

and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

   9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

   10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

   11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

  12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

  13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

  14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

                              NO WARRANTY

  15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

  16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUD-

ING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

    <one line to give the library's name and a brief idea of what it does.>

    Copyright (C) <year> <name of author>

    This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

    This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

    You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990

  Ty Coon, President of Vice

That's all there is to it!

8.4.3   Libpcap

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

8.4.4 OpenSSL

```
LICENSE ISSUES
===============
```

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

```
OpenSSL License
----------------
```

```
/* ====================================================================
 * Copyright (c) 1998-2005 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
```

```
 *      acknowledgment:
 *      "This product includes software developed by the OpenSSL Project
 *      for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ======================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
Original SSLeay License
-----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given
 * attribution as the author of the parts of the library used.
```

```
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *     "This product includes cryptographic software written by
 *      Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *     being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *     the apps directory (application code) you must include an
 *     acknowledgement: "This product includes software written by Tim Hudson
 *     (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

8.4.5   Net-SNMP

Various copyrights apply to this package, listed in various separate parts
below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

        Copyright 1989, 1991, 1992 by Carnegie Mellon University

        Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

                        All Rights Reserved

Permission to use, copy, modify and distribute this software and its docu-
mentation for any purpose and without fee is hereby granted, provided that
the above copyright notice appears in all copies and that both that copyright
notice and this permission notice appear in supporting documentation, and
that the name of CMU and The Regents of the University of California not be
used in advertising or publicity pertaining to distribution of the software
without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANT-
ABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY
OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES
OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARIS-
ING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modifica-
tion, are permitted provided that the following conditions are met:

*   Redistributions of source code must retain the above copyright notice,
    this list of conditions and the following disclaimer.

*   Redistributions in binary form must reproduce the above copyright notice,
    this list of conditions and the following disclaimer in the documentation
    and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names
  of its contributors may be used to endorse or promote products derived
  from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS''
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSE-
QUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAM-
AGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modifica-
tion, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote
  products derived from this software without specific prior written per-
  mission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN
NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, IN-
CIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA,
OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLI-
GENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*   Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

*   Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

*   Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSE-QUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAM-AGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2007, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*   Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be
  used to endorse or promote products derived from this software without
  specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS''
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSE-
QUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAM-
AGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modifica-
tion, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecom-
  munications, nor the names of their contributors may be used to endorse
  or promote products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS''
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSE-
QUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8.4.6   Zlib

ZLIB DATA COMPRESSION LIBRARY

zlib 1.2.3 is a general purpose data compression library. All the code is thread safe. The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files

http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format). These documents are also available in other formats from ftp://ftp.uu.net/graphics/png/documents/zlib/zdoc-index.html

All functions of the compression library are documented in the file zlib.h
(volunteer to write man pages welcome, contact zlib@gzip.org). A usage exam-
ple of the library is given in the file example.c which also tests that the
li-brary is working correctly. Another example is given in the file minigz-
ip.c. The compression library itself is composed of all source files except
exam-ple.c and minigzip.c.

To compile all files and run the test program, follow the instructions given
at the top of Makefile. In short "make test; make install" should work for
most machines. For Unix: "./configure; make test; make install". For MSDOS,
use one of the special makefiles such as Makefile.msc. For VMS, use
make_vms.com.

Questions about zlib should be sent to <zlib@gzip.org>, or to Gilles Vollant
<info@winimage.com> for the Windows DLL version. The zlib home page is http:/
/www.zlib.org or http://www.gzip.org/zlib/ Before reporting a problem,
please check this site to verify that you have the latest version of zlib;
otherwise get the latest version and check whether the problem still exists
or not.

PLEASE read the zlib FAQ http://www.gzip.org/zlib/zlib_faq.html before ask-
ing for help.

Mark Nelson <markn@ieee.org> wrote an article about zlib for the Jan. 1997
issue of Dr. Dobb's Journal; a copy of the article is available in http://
dogma.net/markn/articles/zlibtool/zlibtool.htm

The changes made in version 1.2.3 are documented in the file ChangeLog.

Unsupported third party contributions are provided in directory "contrib".

A Java implementation of zlib is available in the Java Development Kit http:/
/java.sun.com/j2se/1.4.2/docs/api/java/util/zip/package-summary.html
See the zlib home page http://www.zlib.org for details.

A Perl interface to zlib written by Paul Marquess <pmqs@cpan.org> is in the
CPAN (Comprehensive Perl Archive Network) sites http://www.cpan.org/modules/
by-module/Compress/

A Python interface to zlib written by A.M. Kuchling <amk@amk.ca> is available
in Python 1.5 and later versions, see http://www.python.org/doc/lib/module-
zlib.html

A zlib binding for TCL written by Andreas Kupries <a.kupries@westend.com> is availlable at http://www.oche.de/~akupries/soft/trf/trf_zip.html

An experimental package to read and write files in .zip format, written on top of zlib by Gilles Vollant <info@winimage.com>, is available in the contrib/minizip directory of zlib.

Notes for some targets:

- For Windows DLL versions, please see win32/DLL_FAQ.txt

- For 64-bit Irix, deflate.c must be compiled without any optimization. With -O, one libpng test fails. The test works in 32 bit mode (with the -n32 compiler flag). The compiler bug has been reported to SGI.

- zlib doesn't work with gcc 2.6.3 on a DEC 3000/300LX under OSF/1 2.1 it Works when compiled with cc.

- On Digital Unix 4.0D (formely OSF/1) on AlphaServer, the cc option -std1 is necessary to get gzprintf working correctly. This is done by configure.

- zlib doesn't work on HP-UX 9.05 with some versions of /bin/cc. It works with other compilers. Use "make test" to check your compiler.

- gzdopen is not supported on RISCOS, BEOS and by some Mac compilers.

- For PalmOs, see http://palmzlib.sourceforge.net/

- When building a shared, i.e. dynamic library on Mac OS X, the library must be installed before testing (do "make install" before "make test"), since the library location is specified in the library.

Acknowledgments:

  The deflate format used by zlib was defined by Phil Katz. The deflate and zlib specifications were written by L. Peter Deutsch. Thanks to all the people who reported problems and suggested various improvements in zlib; they are too numerous to cite here.

Copyright notice:

 (C) 1995-2004 Jean-loup Gailly and Mark Adler

  This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

```
Jean-loup Gailly          Mark Adler
jloup@gzip.org            madler@alumni.caltech.edu
```

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes. Please read the FAQ for more information on the distribution of modified source versions.

8.4.7 Mini Httpd

Copyright © 1999, 2000 by Jef Poskanzer <jef@acme.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without modificati-on, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EX-PRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WAR-RANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DIS-CLAI-MED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DI-RECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (IN-CLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLI-GENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8.4.8   Ipsec Tools

The ipsec-tools uses the 3 clause BSD license and the follow X11-License

```
# This originates from X11R5 (mit/util/scripts/install.sh), which was
# later released in X11R6 (xc/config/util/install.sh) with the
# following copyright and license.
#
# Copyright (C) 1994 X Consortium
#
# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to
# deal in the Software without restriction, including without limitation the
# rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
# sell copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in
# all copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN
# AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNEC-
# TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
#
# Except as contained in this notice, the name of the X Consortium shall not
# be used in advertising or otherwise to promote the sale, use or other deal-
# ings in this Software without prior written authorization from the X Consor-
# tium.
```

8.4.9 OpenSSH

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)

```
 * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
 *                     All rights reserved
 *
 * As far as I am concerned, the code I have written for this software
 * can be used freely for any purpose.  Any derived versions of this
 * software must be clearly marked as such, and if the derived work is
 * incompatible with the protocol description in the RFC file, it must be
 * called by a name other than "ssh" or "Secure Shell".


 [Tatu continues]
 *  However, I am not implying to give any licenses to any patents or
 * copyrights held by third parties, and the software includes parts that
 * are not under my direct control.  As far as I know, all included
 * source code is used in accordance with the relevant license agreements
 * and can be used freely for any purpose (the GNU license being the most
 * restrictive); see below for details.


 [However, none of that term is relevant at this point in time.  All of
 these restrictively licenced software components which he talks about
 have been removed from OpenSSH, i.e.,

 - RSA is no longer included, found in the OpenSSL library

 - IDEA is no longer included, its use is deprecated

 - DES is now external, in the OpenSSL library

 - GMP is no longer used, and instead we call BN code from OpenSSL

 - Zlib is now external, in a library

 - The make-ssh-known-hosts script is no longer included

 - TSS has been removed

 - MD5 is now external, in the OpenSSL library

 - RC4 support has been replaced with ARC4 support from OpenSSL

 - Blowfish is now external, in the OpenSSL library
```

```
[The licence continues]
```

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

   The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

   * Cryptographic attack detector for ssh - source code
   *
   * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
   *
   * All rights reserved. Redistribution and use in source and binary
   * forms, with or without modification, are permitted provided that
   * this copyright notice is retained.
   *

```
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
* WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
* CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
* SOFTWARE.
*
* Ariel Futoransky <futo@core-sdi.com>
* <http://www.core-sdi.com>
```

3)

```
  ssh-keyscan was contributed by David Mazieres under a BSD-style license.


    * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
    *
    * Modification and redistribution in source and binary forms is
    * permitted provided that due credit is given to the author and the

    * OpenBSD project by leaving this copyright notice intact.
```

4)
```
  The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo
  Barreto is in the public domain and distributed with the following li-
  cense:


    * @version 3.0 (December 2000)
    *
    * Optimised ANSI C code for the Rijndael cipher (now AES)
    *
    * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
    * @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
    * @author Paulo Barreto <paulo.barreto@terra.com.br>
    *
    * This code is hereby placed in the public domain.
    *
    * THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS
    * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
    * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
    * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
    * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
    * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
    * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
```

```
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
* OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
* EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

```
* Copyright (c) 1983, 1990, 1992, 1993, 1995
*      The Regents of the University of California.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*     without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
* BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
* SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
* INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
* CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF
* THE POSSIBILITY OF SUCH DAMAGE.
```

6)

Remaining components of the software are provided under a standard

2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos

Dug Song

Aaron Campbell

Damien Miller

Kevin Steves

Daniel Kouril

Wesley Griffin

Per Allansson

Nils Nordman

Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom

Tim Rice

Andre Lucas

Chris Adams

Corinna Vinschen

Cray Inc.

Denis Parker

Gert Doering

Jakob Schlyter

Jason Downs

Juha Yrjölä

Michael Stone

Networks Associates Technology, Inc.

Solar Designer

Todd C. Miller

Wayne Schroeder

William Jones

Darren Tucker

Sun Microsystems

The SCO Group

Daniel Walsh

    * Redistribution and use in source and binary forms, with or without

    * modification, are permitted provided that the following conditions

    * are met:

    * 1. Redistributions of source code must retain the above copyright

    *   notice, this list of conditions and the following disclaimer.

    * 2. Redistributions in binary form must reproduce the above copyright

    *   notice, this list of conditions and the following disclaimer in the

    *   documentation and/or other materials provided with the distribution.

    *

    * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR

   * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES

    * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

    * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,

   * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

   * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,

    * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

    * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

    * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF

    * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

    a) md5crypt.c, md5crypt.h

* "THE BEER-WARE LICENSE" (Revision 42):

```
* <phk@login.dknet.dk> wrote this file.  As long as you retain this
* notice you can do whatever you want with this stuff. If we meet
* some day, and you think this stuff is worth it, you can buy me a
* beer in return.   Poul-Henning Kamp


  b) snprintf replacement
* Copyright Patrick Powell 1995
* This code is based on code written by Patrick Powell
* (papowell@astart.com) It may be used for any purpose as long as this
* notice remains intact on all source code distributions


  c) Compatibility code (openbsd-compat)
      Apart from the previously mentioned licenses, various pieces of code
      in the openbsd-compat/ subdirectory are licensed as follows:
      Some code is licensed under a 3-term BSD license, to the following
      copyright holders:
Todd C. Miller
Theo de Raadt
Damien Miller
Eric P. Allman
The Regents of the University of California
Constantin S. Svintsoff


* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
```

```
* 3. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
* BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
* SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
* INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
* CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF
* THE POSSIBILITY OF SUCH DAMAGE.


        Some code is licensed under an ISC-style license, to the following
        copyright holders:


Internet Software Consortium.

Todd C. Miller

Reyk Floeter

Chad Mynhier


* Permission to use, copy, modify, and distribute this software for any
* purpose with or without fee is hereby granted, provided that the above
* copyright notice and this permission notice appear in all copies.
*
* THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL
* WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE
```

```
* LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR
* ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
* WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION,
* ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
* SOFTWARE.


        Some code is licensed under a MIT-style license to the following
        copyright holders:
Free Software Foundation, Inc.


* Permission is hereby granted, free of charge, to any person obtaining a
* copy of this software and associated documentation files (the
* "Software"), to deal in the Software without restriction, including
* without limitation the rights to use, copy, modify, merge, publish,
* distribute, distribute with modifications, sublicense, and/or sell
* copies of the Software, and to permit persons to whom the Software is
* furnished to do so, subject to the following conditions:
*
* The above copyright notice and this permission notice shall be included
* in all copies or substantial portions of the Software.
*
* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
* OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
* MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
* IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
* DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
* OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR
* THE USE OR OTHER DEALINGS IN THE SOFTWARE.
*
* Except as contained in this notice, the name(s) of the above copyright
* holders shall not be used in advertising or otherwise to promote the
```

```
* sale, use or other dealings in this Software without prior written

* authorization.


------

$OpenBSD: LICENCE,v 1.19 2004/08/30 09:18:08 markus Exp $
```

8.4.10   JSON-C

```
X11 like License
```

```
Copyright (c) 2004, 2005 Metaparadigm Pte Ltd
```

```
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is fur-
nished to do so, subject to the following conditions:
```

```
The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.
```

```
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE

SOFTWARE.
```

8.4.11   lsof License

```
Warranty
```

```
========
```

```
Lsof is provided as-is without any warranty of any kind, either expressed or
implied, including, but not limited to, the implied warranties of merchant-
ability and fitness for a particular purpose. The entire risk as to the qual-
ity and performance of lsof is with you.  Should lsof prove defective, you
assume the cost of all necessary servicing, repair, or correction.
```

```
License
========

Lsof has no license.  Its use and distribution are subject to these terms and
conditions, found in each lsof source file.  (The copyright year in or format
of the notice may vary slightly.)

    /*

     * Copyright 2002 Purdue Research Foundation, West Lafayette,

     * Indiana 47907.  All rights reserved.

     *

     * Written by Victor A. Abell

     *

     * This software is not subject to any license of the American

     * Telephone and Telegraph Company or the Regents of the

     * University of California.

     *

     * Permission is granted to anyone to use this software for

     * any purpose on any computer system, and to alter it and

     * redistribute it freely, subject to the following

     * restrictions:

     *

     * 1. Neither the authors nor Purdue University are responsible

     *    for any consequences of the use of this software.

     *

     * 2. The origin of this software must not be misrepresented,

     *    either by explicit claim or by omission.  Credit to the

     *    authors and Purdue University must appear in documentation

     *    and sources.

     *

     * 3. Altered versions must be plainly marked as such, and must

     *    not be misrepresented as being the original software.

     *

     * 4. This notice may not be removed or altered.

     */
```

8.4.12 MIT License

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

8.4.13 8.4.13 file-4.19

$Id: LEGAL.NOTICE,v 1.15 2006/05/03 18:48:33 christos Exp $

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others;

maintained 1994- Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index